Revolução Satoshi

A Revolução das Esperanças Crescentes

Revolução Satoshi

A Revolução das Esperanças Crescentes

Escrito por
Wendy McElroy

1ª edição

Sumário

Agradecimentos 9
Prefácio, por Jeffrey A. Tucker 11
A Regulação é a Chave 12
Quanto Tempo Vai Demorar? 13
Um Mundo Criptonizado 14
Forçando o Passado no Presente 15
Introdução 17
Liberdade Versus Poder 17
A Revolução sem Sangue 21
O Poder do Peer-to-Peer 23
A Necessidade de um Dinheiro Descentralizado 26
O Primado da Privacidade 29
Conclusão 30

Seção Um. O Problema da Terceira Parte Confiável 33
Capítulo Um. Ouvindo o Passado 35
Precedentes na Teoria Individualista Radical 37
A América nasceu na moeda privada 41
Como e por que o governo proibiu o dinheiro privado 43
O Teorema da Regressão 49
O Dinheiro pode criar Libertação e Civilização […] ou Opressão 53
Um Breve Tour Pelo Básico 55
Inflação, o Maior Roubo de Todos 57
Liberdades Civis e Bancos Centrais 61
Capítulo Dois. A Tecnologia Encontra a Anarquia, e Ambos Lucram 65
A História do Bitcoin 66
Levantem-se, Cypherpunks! 68
As Guerras Cripto Continuam 71
Lições de Moral de Moedas Digitais Anteriores 73
Capítulo Três. Descobrindo Satoshi 81
Satoshi e Buckminister Fuller 82
Satoshi é um Libertário e Anarquista? 87
Evidência das motivações políticas de Satoshi 89

Evidências a partir do “White Paper” 90
Evidência a partir de postagens e associações pessoais 93
Evidência do ambiente de Satoshi 95
Legado de Satoshi 96
Capítulo Quatro. O Governo Leva a Cripto a Sério 99
Uma estratégia do estado para controlar a cripto 99
O que é a S.1241? 101
Protegendo as pessoas de sua liberdade 105
Uma segunda estratégia de controle: Cripto emitida pelo governo 107
Por que o impulso para uma sociedade sem dinheiro? 109
A estratégia das corretoras centralizadas 112

Seção Dois. O Imperativo da Privacidade 119
Capítulo Cinco. Quando a Privacidade é Criminalizada, Apenas os Criminosos têm Privacidade 121
O que é Privacidade? 121
O contexto dos direitos humanos à privacidade 123
Uma mudança dramática no paradigma da privacidade 127
O valor da privacidade para a sociedade 134
Capítulo Seis. Nomes Verdadeiros e Estratégias para a Privacidade 141
A origem dos True Names 142
Sistemas offline de identificação de livre mercado 144
Objeções ao ID de livre mercado 148
O que você deveria fazer? 151

Seção Três. Descentralização 157
Capítulo Sete. Descentralização no Núcleo da Cripto-Liberdade 159
O que é Centralização? O que é Descentralização? 159
O Novo Individualismo Austríaco 165
Ordem Espontânea na Produção Econômica 170
Capítulo Oito. A Cripto Como um Fenômeno Econômico Austríaco 175
A Cripto-Cataláxia 175
Os Aspectos Revolucionários Não Reconhecidos da Cripto ... 179
Descentralização como Desobediência 182
Anarquismo: o Ponto Final da Descentralização 187

O que é o Anarquismo Individualista ou Libertário?...............190
Uma Saudação a Henry David Thoreau..................................192

Seção Quatro. Estado e Sociedade 195
Capítulo Nove. Relevância do Estado, da Sociedade e da Obediência para a Cripto 197
A Estrutura do estado, da Sociedade e das criptomoedas 197
O estado Contra a Sociedade 204
As teorias do consentimento e da conquista do estado 208
Servidão Voluntária...211
Estado, Sociedade, Obediência e Cripto 216
Capítulo Dez. Teoria Cripto de Classe e Lei de Livre Mercado...219
Guerra de Classes e Cripto...219
A aplicação da lei como ferramenta da guerra de classes 222
Lei de livre mercado 223
A Primeira Discussão da Lei de Livre Mercado e Sistemas de Defesa 225
Locke sobre o argumento do consenso para o direito..............228
Segurança preventiva..232
Uma Pergunta Assombrosa...233

Seção Cinco. Cripto, Lei e Justiça 235
Capítulo Onze. Lidando com o Crime sem o Estado 237
Comparado ao que? 237
O estado destrói o que não pode controlar...............................239
O que é Justiça? 243
Os Requisitos do Direito de Contratos Privados 246
A razão pela qual a aparência futura da justiça proprietária é imprevisível 251
Rumo a uma nova visão de justiça..252
Considere a dinâmica de um crime específico: A Fraude 257
Uma Revolução Prática e Descentralizada 260
Posfácio 263

Agradecimentos

Primeiro e antes de tudo, eu gostaria de agradecer a Roger Ver pela confiança que ele depositou em *A Revolução Satoshi* e pela generosidade com a qual ele trata a mim e a todos os outros com quem ele trabalha. Ele é o tipo mais raro de visionário; um que traduz sua visão na realidade.

Pessoas demais no Bitcoin.com ajudaram na serialização de uma versão inicial de *A Revolução Satoshi* para que eu possa listá-las, mas algumas não podem passar sem menção. Mate Tokay é um coordenador magistral para todas as coisas no bitcoin.com e o responsável por preservar tanto o contexto amplo da operação bem como suas minúcias. As décadas do Editor-Chefe Nanok Bie no jornalismo foram inestimáveis. Marcel Chou é um editor paciente que se tornou um amigo e porta-voz confiável. Aqueles que eu cheguei a chamar de “The Bitcoin Guys”, nem uma vez tentaram influenciar as teorias sendo testadas e as hipóteses sendo publicadas. Sou grata a todos eles.

Jeff Tucker, autor do Prefácio, tem sido para mim um associado altamente estimado por muitos anos; ele não poderia ter sido mais encorajador com os artigos na medida em que eles apareceram. Para seu crédito, Jeff captou mais rápido do que eu as implicações extraordinárias que as criptomoedas têm para a liberdade. Minha evolução nesse entendimento também possui uma dívida com uma quantidade muito numerosa de pessoas para listar. O mais proeminente entre eles é o notável advogado de propriedade intelectual Stephan Kinsella e o Presidente do Satoshi Nakamoto Institution, Michael Goldstein.

Eu tive outra sorte grande durante *A Revolução Satoshi*. Repentinamente, a Dra. Peri Dwyer-Worrell me mandou um e-mail com uma oferta para revisar meus artigos. Eu sempre fui indiferente em assuntos tais como a colocação de vírgulas, carregando comigo a crença de que apenas as ideias são importantes. Peri provou que eu estava errada e, no processo, ela me fez uma escritora. Eu estou muito agradecida por finalmente ter cuidado com a pontuação e por conhecer essa elegante mulher.

Nenhuma dedicatória estaria completa sem uma expressão de meus agradecimentos eternos a Bradford, meu marido, que é o pilar indispensável para tudo o que eu faço.

Prefácio

O mundo tem precisado desse livro para que tenhamos a visão geral da revolução que está ocorrendo, e Wendy McElroy é a pessoa exata para escrever isso. Seu trabalho tem sido imerso na história da liberdade e da luta contra o controle autoritário. Ela traçou essa luta desde o século XIX até o presente, tendo escrito artigos pioneiros e livros contemplando a amplitude da experiência humana. Em *A Revolução Satoshi*, ela voltou a atenção dela ao que estou convencido ser uma das inovações mais memoráveis da história: criptomoedas, ativos e serviços relacionados. Ela explica como, em nosso próprio tempo, essa tecnologia pressagia mudanças fundamentais, grandes mudanças, na relação entre o indivíduo e o estado. Nos últimos dez anos – historiadores futuros notarão isso – observamos a criação de uma nova arquitetura monetária e financeira que poderá servir como uma substituição para tudo que tem sido conhecido e usado no tempo de vida de todas as pessoas hoje presentes.

Experienciamos um dinheiro seguro e útil que funciona em todo o mundo, não é conectado ao estado, e não precisa do atual sistema bancário. O mesmo sistema pode servir como substituição a todo sistema atual de pagamentos que usam moedas nacionais. Esse dinheiro é uma criação puramente mercadológica que adiciona às funções de contabilidade e de reserva de valor uma característica adicional: ser também um meio de pagamento global peer-to-peer.

Uma década atrás, até mesmo teóricos de alto nível disseram que isso não poderia acontecer. E então aconteceu.

Vimos a criação de um sistema de contratos inteligentes, que pode gerenciar um vasto número de acordos, comprometimentos e interações humanas. Até mesmo pessoas que aceitaram que o Bitcoin era real duvidaram que a Ethereum poderia alcançar isso. Mas isso aconteceu de qualquer forma.

Nós até observamos como esse sistema se tornou um instrumento para levantar capital e substituir as funções de empréstimo tradicionais. Três anos atrás, isso era meramente uma ideia especulativa. Então isso se tornou uma realidade de cem bilhões de dólares, e novas formas de capital estão sendo levantadas através da tokenização.

Aparentemente do nada, temos agora todo um conjunto de tecnologias que poderiam concebivelmente deslocar e até mesmo substituir a moeda nacional, opções de pagamento tradicionais, e até mesmo mercados de capitais regulados, e trazer algo novo.

Você está lendo isso e pensando: aqui vamos nós de novo com o cripto-utopismo. Mas esse é o pulo do gato: não é mais apenas teoria. Essas tecnologias existem, ao vivo e em cores, mesmo que estejam em seus estágios iniciais. É por isso que há tantos bitcoiners por aí que falam tão exuberantemente sobre o futuro. Eles já experimentam isso. Eles são motoristas de Maseratis em estradas cheias de Ford T's, e eles sabem disso. Uma melhoria do status quo que é tão impressionante que não será suprimida.

Você pode não ter usado qualquer uma dessas novas tecnologias. E está tudo bem. Com todas as falhas do atual sistema, as antigas estruturas cumprem seu trabalho. Na medida em que não há uma grande crise no sistema, as pessoas confiam nele. Não há razões fortes para mudar, mesmo que o novo sistema seja mais seguro, mais rápido, mais democrático, mais inclusivo e menos arriscado e comprometedor da privacidade individual. Ainda assim, o antigo sistema goza do ímpeto que vem a partir do efeito manada. Todo mundo confia no antigo sistema, então você continua confiando nele também.

A Regulação é a Chave

Há outro fator que está atrasando a mudança do antigo para o novo. As regulações estão tentando forçar a nova tecnologia a se comportar como a tecnologia antiga. Nos Estados Unidos, para comprar Bitcoin ou qualquer criptomoeda, você precisa cumprir com regulações know-your-customer, cedendo cada detalhe sobre a sua pessoa. Qualquer dinheiro que você faça de movimentos dos preços em ascensão em um novo ativo precisa ser registrado e você precisa pagar impostos sobre ele. Companhias que desejam prestar assistência no onboarding e no offboarding de cripto para moeda fiduciária têm de se registrar no governo como casas de câmbio. E, com as funções de alavancamento de capital da tecnologia blockchain, os reguladores estão ameaçando acabar com todas e fazê-las se comportar como títulos tradicionais.

Eu assisti enquanto essas regulações, gradualmente impostas e arbitrariamente reforçadas, introduziram um elemento de medo em uma

tecnologia sem medo, distorcendo o setor e fazendo dele menos inovador e menos competitivo. Toda vez que um novo uso das redes distribuídas é revelado e começa a se espalhar, alguns mandachuvas surgem do alto para advertir sobre a conformidade com leis de décadas atrás designadas para diferentes tecnologias.

Os consumidores ficam com medo, e a experiência de usuário final não é aprimorada o tanto quanto ela poderia ter sido na ausência de tantos custos de compliance. Eu vi o quanto a incerteza legal fez com que os mercadores e os consumidores perdessem acesso a uma variedade de serviços. Eu vi empreendedores interromperem seus planos, esperando algum édito administrativo vindo de Washington, DC.

O quão mais avançados estaríamos no caso da ausência dessas regulações? É impossível ver as inovações que não experienciamos. Sabemos apenas que as coisas seriam diferentes. Mas uma vez que você considera o quão diferente seriam, a realidade se torna algo além do incrível. E ainda não chegamos nisso.

Quanto Tempo Vai Demorar?

Considere o que acontece quando o poder é usado para parar o progresso de uma nova tecnologia. Isso realmente funcionaria no longo prazo? Para responder à questão, temos de nos engajar nos contrafactuais.

Imagine se os governos na Europa tivessem se empenhado para parar a prensa. E se as cidades ao redor do mundo tivessem banido os automóveis? Qual teria sido o destino das ferrovias, da iluminação doméstica e do encanamento fechado se interesses especiais houvessem sido suprimidos em favor das tecnologias prevalecentes?

Podemos apenas especular, porque nada disso realmente aconteceu. É verdade que nem todo mundo recebeu bem a prensa. Escribas em monastérios se preocuparam com o futuro de seus talentos. Algumas pessoas perguntaram se a velha fé poderia sobreviver às pessoas tendo acesso aos textos antigos. Mas, em geral, o advento da prensa foi visto como uma inovação bem-vinda. Assim também se deu com a combustão interna, eletricidade e encanamento. Algumas pessoas ficaram receosas em adotar elas, é claro, mas os governos em sua maioria deixaram a inovação acontecer.

E se eles não tivessem? Alguém realmente acredita que essas inovações poderiam ser paradas e não meramente atrasadas? Eu penso que

não. Há casos na história em que garantias de monopólios por parte do governo retardam competidores de adentrarem no mercado com melhorias. Isso aconteceu com os navios a vapor na Inglaterra, com os aviões nos EUA, e com algumas aplicações de software nas últimas décadas. Mas esses retardamentos são temporários; patentes expiram e a história vai para frente.

Regulações são diferentes. Os empreendedores têm de inovar ao redor delas. Os mercados cinza e negro emergem. Aventureiros encaram as autoridades. Mas, eventualmente, alguém cede. Considere, por exemplo, os resultados caso todo lorde e barão na Europa do século XII tivesse banido a ferradura. Você acha que isso teria parado a implementação dessa tecnologia por séculos? Altamente duvidoso, e a razão é fundamental: ideias são mais fortes que governos. Eventualmente, os custos de imposição excedem vastamente os benefícios da classe governante existente.

Um Mundo Criptonizado

À luz do que temos visto nos últimos dez anos, aqui está um experimento mental com o qual eu venho brincando. Ele ocorreu a mim numa divagação, enquanto meu advogado tributário estava explicando-me profundamente sobre eventos tributáveis nos acordos cotidianos com cripto. Eu estava considerando o quão incompatíveis eram essas imposições com uma tecnologia que emergiu de e opera dentro de uma estrutura de perfeita liberdade.

Algumas legislações entenderam isso. O Wyoming, por exemplo, isentou a cripto de toda tributação, definiu certos tokens de um modo que faz deles isentos de leis de títulos, e fizeram provisões especiais para formas corporativas que são distribuídas, entre outras mudanças. A legislação fez o seu melhor para tornar o estado atrativo para essa nova indústria.

Agora, deixe-nos entrar no campo da fantasia. Digamos que o congresso dos EUA passe uma legislação que isente toda criptomoeda, todo criptotrading e criptoativos de toda tributação e regulação. A legislação estabeleceria laissez-faire completo nesse setor, enquanto todo o resto no mundo normal (o dólar, o FED, a SEC, o Tesouro, e todo o resto que conhecemos) permaneceria o mesmo.

O que você acha que aconteceria? Dez anos atrás, se o Congresso tivesse feito a mesma coisa, pouca coisa teria mudado, obviamente. A

tecnologia não existia, e nós realmente não sabíamos que ela poderia existir.

O que aconteceria hoje se todas as intervenções ao redor dessa tecnologia fossem repelidas? Você não seria mais punido por comprar e vender em cripto, emitir novos tokens, desenvolver novos aplicativos em plataformas de contratos inteligentes, inovar novos sistemas de pagamentos e assim em diante. Companhias poderiam tokenizar em vez de vender ações. Os negócios poderiam pagar em cripto e fazer sua contabilidade em cripto e evitar qualquer penalidade. Considere com cuidado: você poderia manter um terço a mais dos seus ganhos justos simplesmente mudando para uma tecnologia melhor.

Quanto tempo levaria para a criptoeconomia substituir todo o resto? Se essa mudança legislativa realmente acontecesse – e não, obviamente não vai – poderíamos observar o deslocamento geral dos sistemas econômicos e financeiros do velho mundo para os sistemas do século XXI, e talvez isso acontecesse muito mais cedo do que qualquer poderia esperar, talvez de 12 a 48 meses, dado que a infraestrutura da cripto poderia escalar a tempo de satisfazer a nova demanda.

Forçando o Passado no Presente

Agora, se esse experimento mental estiver correto, há algumas implicações poderosas. Isso sugere que o mundo financeiro e monetário, tal como existe hoje, está sendo mantido de pé pela força que está nos prendendo aos velhos modos. Essa força está impondo limitações e ineficiências; ela está literalmente mantendo uma vasta infraestrutura no lugar daquilo que de outro modo cessaria de dominar ou até de existir, e impedindo o início de um novo modo de viver. E esse novo modo não é somente sobre comprar e vender. Tão central para nossas vidas públicas são a moeda nacionalizada e os mercados de capital regulados que o advento de um mundo criptonizado mudaria fundamentalmente a relação do indivíduo com o estado.

Estaria eu errado em estar maravilhado com essa percepção?

Manter um sistema vasto vivo apenas pela força não me parece tão sustentável no longo prazo. Se você possui um conjunto massivo de tecnologias que estão esperando para assumir o controle e estão apenas sendo atrasadas por meios puramente artificiais, esse cenário não parece sustentável dada a improbabilidade de que o passado possa para sempre

ser preservado. O futuro não pode para sempre ser adiado mesmo pelos governos mais poderosos do mundo. Eventualmente as ideias vencem.

Wendy McElroy, a partir de seus estudos passados de história e de seu mergulho profundo na cripto-tecnologia, entende o poder dessas ideias. O Bitcoin e tudo que é relacionado a ele estão entre as ideias mais revolucionárias da história. Ela demonstra como eles vão transformar para melhor a estrutura da economia, da política, e das relações humanas num geral. Ir daqui para lá requer o entendimento mais amplo possível do que está acontecendo. McElroy é a guia expert e erudita pela qual estávamos esperando.

Jeffrey A. Tucker é Diretor Editorial do American Institute For Economic Research e antigo Diretor de Conteúdo pela Foundation for Economic Education. Ele é parceiro de gestão da Vellum Capital: Blockchain Financial Management, fundador da Liberty.me, Membro Honorário Distinto do Mises Brasil, conselheiro econômico da FreeSociety.com, companheiro de pesquisa no Acton Institute, conselheiro político do Heartland Institute, fundador da CryptoCurrency Conference, membro da bancada editorial da Molinari Review, um conselheiro para a desenvolvedor de aplicativos blockchain Factom. Ele é o autor de milhares de artigos na imprensa acadêmica e popular e é autor de oito livros em oito línguas, o mais recente sendo *The Market Loves You*. Ele fala amplamente sobre economia, tecnologia, filosofia social, e cultura.

"Você nunca muda as coisas lutando contra a realidade existente. Para mudar algo, construa um novo modelo que faça o modelo existente obsoleto."
– R. Buckminster Fuller

A revolução de 2009 passou despercebida pela maioria das pessoas porque ela foi pacífica, ordenada, e tecnologicamente arcana. Em 2009, Satoshi Nakamoto lançou um software de código aberto por meio do qual transferências peer-to-peer de riqueza digital, chamada bitcoins, cintilaram através de um registro imutável e transparente, chamado blockchain.

O modelo mais conhecido de revolução é a derrubada de um governo opressor por meio de uma revolta popular. Mas a dura realidade da história é que outro governo quase inevitavelmente surge como uma substituição – um governo tão elitista e brutal quanto seu predecessor. O modelo Satoshi de revolução é diferente. Ele pacificamente faz com que o sistema antigo se torne irrelevante ao superá-lo através de uma nova tecnologia e de uma moeda privada diferente de tudo antes visto. A criptomoeda se move ininterruptamente pelo mundo sem estados ou fronteiras, obedecendo apenas aos comandos de indivíduos que escolhem fazer acordos uns com os outros. Transferências são pseudônimas com substancial privacidade providenciada por algoritmos de encriptação e por funções hash. A blockchain é imutável e visível para todos, o que faz dela imune à corrupção. Resistente a manipulação e a inflação pelo governo, a cripto não serve elites poderosas às custas das pessoas comuns. O bitcoin, a cripto, em geral, é o dinheiro do povo. (Nota: O Bitcoin com b maiúsculo denota tanto a moeda quanto a blockchain; bitcoin denota a moeda).

Em um instante, com a primeira faísca de transferência, o mundo mudou para sempre.

Liberdade Versus Poder

Os indivíduos subitamente tiveram a arma de autodefesa que estava faltando no arsenal deles – uma arma que era necessária para vencer o que o economista austríaco Murray Rothbard chama de “o grande conflito que é travado eternamente entre a Liberdade e o Poder”. Os indivíduos ganharam uma moeda privada viável que os permitiu controlar suas próprias riquezas e se tornarem seus próprios bancos – serem “selfbanks”. Finalmente houve um caminho prático para longe da moeda fiduciária manipulada e das instituições financeiras corruptas que formam a base do poder estatal. (As palavras “estado” e “governo” são usadas intercambiavelmente neste livro).

O Bitcoin chegou no momento certo. Apenas dois anos antes, o monopólio monetário causou a crise financeira de 2007-2008 em todo o globo. O Bitcoin e a blockchain ofereceram aos indivíduos um sistema melhor – um que serviu às necessidades deles, não àquelas da elite, e prometeu a independência financeira e controle, os fundamentos da autonomia.

Em sua massiva obra *Conceived in Liberty* (Volume 2), Rothbard apresenta uma visão ampla do porquê dessa libertação ser essencial. Ela não é somente “um grande bem moral em si mesmo”, mas também “a condição necessária para o florescimento de todos os outros bens pelos quais a humanidade presa: a virtude moral, a civilização, as ciências e as artes e a prosperidade econômica”. Sem uma moeda privada e sem um sistema bancário baseado na Liberdade, não no Poder, o potencial humano estava mutilado.

Até chegar o Bitcoin, entretanto, poucos pré-requisitos de liberdade receberam tanta atenção de ativistas políticos modernos quanto a necessidade por uma moeda privada e por um sistema bancário privado que é acessível a todos. Os guerreiros da liberdade marcharam e morreram sob bandeiras nas quais se liam LIBERDADE, VERDADE e JUSTIÇA. Em nenhuma bandeira que eu me lembre lia-se DINHEIRO PRIVADO, SELF-BANKING, mesmo que esses mecanismos fossem essenciais para cumprir a maioria dos outros objetivos na vida.

(Nota: Dinheiro possui três usos tradicionais: é um meio de troca, uma reserva de valor, e uma unidade de conta. A cripto pode servir às três funções, mas a discussão aqui é limitada à moeda (currency) – o dinheiro em circulação como um meio de troca).

A autonomia econômica é a rocha matriz da libertação sem a qual outros direitos se tornam problemáticos. A liberdade da expressão é irrelevante para um homem morrendo de fome. A liberdade de associação

soa vazia para uma mulher que precisa aguentar abuso físico para alimentar seus filhos. O Devido Processo Legal é irrelevante para alguém que não pode arcar com os medicamentos requeridos para viver mais um dia. A necessidade fundamental para todo ser humano é prover a sua própria sobrevivência. Somente então pode a libertação se seguir, junto "da virtude moral, da civilização, das artes e das ciências".

Por anos, a visão política do indivíduo ou do time conhecido como Satoshi Nakamoto escapou ao radar público. Desenvolvido por cripto-anarquistas e sem ser amparado por decretos do governo ou pela atenção da mídia, as autoridades do estado não notaram o fenômeno, aquelas que o notaram desdenharam dele. Eles notam agora, e seus sorrisos sádicos desapareceram de suas faces. Bancos e negócios agora avidamente adotam e adaptam a blockchain porque eles reconhecem seu incrível poder como ferramenta. Há uma pressa por patentes no que já foi uma comunidade de código aberto. Traders são presos por não serem licenciados. Corretoras são atacadas por não se adequarem à papelada exigida em relação aos consumidores. Os governam clamam para regular a moeda para que se possa controlar não somente seus lucros, mas também o perigo que ela acarreta para seu monopólio sobre o dinheiro.

Rothbard observa, "[A Liberdade] tem sempre sido ameaçada pelas intrusões do poder, o poder que busca suprimir, controlar, aleijar, tributar e explorar os frutos da liberdade e da produção." O poder é também ameaçado pela liberdade porque as duas dinâmicas gozam de uma relação inversa; isto é, enquanto uma cresce, a outra afunda.

Sem dúvida que a visão de Satoshi da libertação individual através da autonomia financeira está sob ataque. Os ataques incluem:

- As criptomoedas são ditas como sendo instrumentos meramente financeiros e como nada sobre as quais se deva estar politicamente entusiasmado. Chamá-las de instrumentos de autodefesa em uma batalha entre Liberdade e Poder é considerado "nonsense anarquista", e a discussão sobre o assunto sequer ocorre.
- Apenas criminosos precisam de privacidade financeira, é dito. Usuários de cripto são traficantes de drogas, sonegadores de impostos, traficantes sexuais e outros similares. De outro modo, por que iriam resistir a se reportarem ao governo? A acusação intimida alguns usuários a permanecerem silenciosos por medo de serem considerados criminosos *a priori*.

- Sem regulação, fraude massiva é dita inevitável. Essa reivindicação diverge a atenção da fraude massiva do sistema fiduciário e do centralismo bancário.

As afirmações precedentes são exemplos dos gravetos que são usados para bater e desacreditar a cripto. Nenhuma delas são válidas, mas muitas são amplamente acreditadas. E as crenças públicas tendem a ser traduzidas em lei sempre que convém ao estado fazer isso.

O ataque mais perigoso à cripto, entretanto, é a "cenoura" – a promessa de respeitabilidade. Até mesmo a comunidade cripto é suscetível a essa tentação. Defensores querem que a blockchain e a cripto sejam tão difundidas quanto possível. Os principais defensores querem aceitação para expandir sobre uma base indivíduo-por-indivíduo, negócio-por-negócio, com todas as interações sendo voluntárias e extralegais. Outros estão menos preocupados com o voluntarismo; eles acreditam que suas reservas e investimentos irão elevar-se em valor se os governos e outras instituições de monopólio se tornarem usuários ou garantidores de segurança. Para esses usuários, a respeitabilidade é a chave para o aumento dos lucros e lucro é tudo. Eles veem defensores que falam sobre a liberdade como obstáculos, instrumentos ou ambos.

Infelizmente, "respeitável" é frequentemente visto como sinônimo para "sancionado pelo estado", quando na verdade os dois termos deveriam ser antônimos. O Bitcoin era necessário precisamente porque instituições do governo e parceiras dele, tais como bancos centrais, são vergonhosas; elas saqueiam as pessoas comuns até os trapos e ossos através de manipulação de moeda, inflação, regulação obstrutiva, impostos e outras artimanhas. As elites botam as pessoas para fora da prosperidade através de licenças, patentes, crédito artificial, restrições de investimento, monopólios e outros obstáculos auto servientes.
Os governos são o problema; eles não são a solução e eles nunca serão. "Sancionado pelo estado" deveria significar "desgraçado", não "respeitável".

Um insulto acrescentado para buscar a sanção do estado é a clara implicação de que a liberdade não é respeitável, que liberdade e respeitabilidade são, de algum modo, antagonistas e requerem o estado como um árbitro. Isso é uma falsa e perigosa dicotomia porque o oposto é verdadeiro, e isso dá ao estado o ponto de apoio por meio do qual se

expande, como sempre acontece. Nada é mais respeitável do que a paisagem de seres humanos fazendo acordos pacificamente uns com os outros visando a vantagem mútua. O que o governo injeta numa sociedade livre é violência ou a ameaça de violência, a qual é o fim da liberdade e da sociedade civil.

As apostas são altas, tanto para a Liberdade quanto para o Poder. Para a Liberdade: Privatizar a sua própria riqueza significa que indivíduos privatizam a vida deles e determinam os termos a partir dos quais eles vivem. Para o Poder: Os governos e as instituições financeiras perdem seu monopólio sobre o dinheiro e sobre a riqueza sem os quais eles são impotentes.

Está na natureza do Poder endurecer suas amarras sempre que ameaçados. O poder irá tentar centralizar, regular, banir ou, de outro modo, dominar as moedas digitais e a blockchain. As tentativas irão falhar, em parte por causa da natureza descentralizada da tecnologia, mas uma grande quantidade de dano pode ser infligida por um estado que falha. A tecnologia não pode ser parada, mas alguns dos indivíduos que a usam podem ser perseguidos, aprisionados e quebrados. A proteção mais certa da vítima é manter clara a visão original de Satoshi sobre a cripto e não se desviar dela.

A Revolução sem Sangue

Essa é a imagem quintessencial da revolução política. Camponeses famintos invadem a Bastilha porque a opressão os moveu para além dos limites da resistência humana. Mas, e se essa imagem estiver errada? Ou lamentavelmente incompleta? E se as forças mais revolucionárias no mundo não forem a fome e o desespero, mas sim a esperança e a oportunidade?

A frase e a dinâmica que captura a última visão é chamada de “a revolução das esperanças crescentes”; ela descreve a promessa mais rígida da revolução Satoshi. O termo tornou-se popular depois que a Segunda Guerra Mundial desestabilizou governos ao redor do globo, com os antigos regimes e sistemas políticos colapsando. A política abomina um vácuo. Especialmente no que era até então chamado de o Terceiro Mundo, as pessoas comuns começaram a acreditar que a vida delas poderia melhorar através de seus próprios esforços. A “revolução das esperanças crescentes” se refere a uma situação na qual um aumento na prosperidade e na liberdade faz as pessoas acreditarem que elas podem

criar uma vida melhor para elas mesmas e para a família delas. Elas não só agem para fazer isso, mas elas também demandam o espaço para respiração política para conseguir mais. Elas têm fome por independência e prosperidade. As esperanças crescentes se tornam uma engrenagem do "populismo" no melhor sentido da palavra.

As autoridades já há muito sabem que um povo oprimido obedece porque eles acreditam que não há alternativa viável. As pessoas acreditam que nenhum ato de resistência pode melhorar a vida delas, então elas mantêm o status quo, por mais sombrio que ele possa ser. A "cinzidade", a conformidade e o medo são os amigos dos regimes totalitários que querem suprimir qualquer faísca de não conformidade ou de criatividade, porque a centelha expressa a escolha individual e a inovação. A centelha não pode ser controlada. Isso é verdade para a esperança. Pessoas esperançosas agem para controlar as suas próprias vidas porque elas vislumbram a possibilidade da libertação e da prosperidade – dois lados da mesma moeda. O sociólogo do século XIX Alexis de Tocqueville observou que a Revolução Francesa foi mais forte em áreas da França onde o padrão de vida havia continuamente evoluído. Foi mais forte lá porque as pessoas acreditaram na possibilidade de continuar a evoluir. Elas esperaram e demandaram.

O conceito de "esperanças crescentes" também explica o porquê de revoltas sociais frequentemente surgirem em locais de oportunidade em vez de em locais de opressão. A revolução flui a partir dos estudantes privilegiados das universidades, por exemplo. Líderes revolucionários notoriamente vêm das classes média ou alta, vêm da intelligentsia, e eles não partilham da vitimidade dos realmente oprimidos que alegam representar. De fato, os oprimidos frequentemente recusam trabalhar pela mudança social. Marx referiu-se a essa categoria da sociedade como o "lumpemproletariado" – o proletariado especificado pelos criminosos, vagabundos e os desempregados, que careciam de consciência [de classe] – ele os escarneceu por não entenderem ou não se importarem com o interesse de sua própria classe. Em vez de esperar por mudança, talvez eles estivessem fazendo o melhor que eles sabiam.

A maioria das revoluções terminam de forma ruim. Algumas começam de forma ruim, com violência e com uma erupção de raiva que parece visar mais a vingança do que a justiça. Até mesmo revoluções inicialmente pacíficas tendem a se dissolver em violência e terminam comandadas por líderes com agendas pessoais – sede de poder, ideologia, ganância, ou todos os fatores acima. Quando a fumaça cessa e os

cadáveres são removidos das ruas, o novo regime é louvado pela população. O novo regime rapidamente revela a si mesmo, entretanto, como sendo não menos tirânico que os tiranos que acabaram de serem destronados.

A Revolução Satoshi não corre esse risco. A blockchain é intrinsecamente pacífica, sem capacidade de cometer violência. A cripto não confronta os governos diretamente, decapita monarcas ou flamulam bastiões da opressão. Ela esquiva e torna-os obsoletos com eficiência brutal. Para aqueles embebidos na versão de revolução que só ergue barricadas, a asserção prévia pode parecer inofensiva. Mas, ao dar às pessoas liberdade financeira – até mesmo uma liberdade incompleta – a cripto é incendiária. O fluxo de trocas e de comércio produz a libertação porque produz a independência e a escolha. Ela estabelece uma revolução de esperanças crescentes que não é baseada em uma ideologia, mas no interesse próprio e racional das pessoas. Nada é mais poderoso.

Mas qual é a engrenagem que move a revolução Satoshi?

O Poder do Peer-to-Peer

O brilhantismo político da cripto reside em um fato: ela resolve o problema da "terceira parte confiável". (Aqui a palavra "confiável" significa o inverso de sua definição literal). Entender esse conceito é essencial para entender como funciona uma sociedade livre. Ainda assim, estava faltando para o léxico da liberdade.

Essa ausência causava estranheza. Depois de tudo, as principais dinâmicas do estado residem em forçar as pessoas a usarem as terceiras partes confiáveis da burocracia e das instituições associadas ao governo como um modo de as controlar. Se as pessoas desejam conduzir a vida cotidiana, elas não têm escolha senão fazer o acordo com as agências monopolistas do estado, incluindo reguladores, agentes de tributação, bancos centrais e impositores da lei. Terceiros confiáveis são o braço de ferro do estado. E é aí onde a parte "problema" do conceito surge. A camada intermediária entre o estado e o povo – a camada das terceiras partes confiáveis – é onde a corrupção e o controle germinam. Ao ordenar o uso dessas partes, o estado consolida sua autoridade e explora a pessoa comum. Sem que a população use suas terceiras partes confiáveis, o estado não tem meios de imposição. A ausência desse conceito é a chave para a ciência política.

A sociedade moderna parece exigir terceiras partes confiáveis, especialmente o sistema bancário central. De outro modo, é argumentado, seres humanos irão retornar às trocas diretas do escambo os quais são desorganizadas e muito limitadas no alcance geográfico do comércio e na variedade de bens trocados.

A cripto e a blockchain conseguiram virar o jogo. O whitepaper original de Satoshi, "Bitcoin: A Peer-to-Peer Cash System" (Outubro de 2008), explica, "O que é necessário é um sistema de pagamento eletrônico baseado em uma prova criptográfica em vez de em confiança, permitindo a quaisquer duas partes querendo transacionar diretamente uma com a outra o façam sem a necessidade de uma terceira parte confiável". Essa é a raison d'être do Bitcoin.

Trata-se de uma questão de perspectiva, entretanto. Há uma função adequada – uma função de livre mercado – para terceiras partes confiáveis. É para facilitar as transações de indivíduos ao providenciar serviços, tais como a verificação de identidade providenciada por um notário. Tais terceiras partes confiáveis são subordinados ao livre mercado ao qual eles existem para servir. Mas até mesmo as terceiras partes confiáveis do livre mercado apresentam problemas. Um é inerente. A palavra "confiado" implica que não é sempre possível verificar se o terceiro é recorrível. Se a verificação fosse possível, então a necessidade de se confiar sequer iria aparecer como um problema; o termo seria "terceira parte verificada". O risco surge em acordos privados, bem como em acordos públicos ou servientes ao estado. Por acaso um advogado opera clandestinamente em nome de si mesmo em vez de em nome de seus clientes, por exemplo? Confiar sua riqueza a outra pessoa é um negócio arriscado, mesmo se você conhecer bem a pessoa. Quando o terceiro é uma instituição impessoal sem contabilidade legal e paga pelo estado, tais como a imposição da lei, o risco aumenta astronomicamente.

Todas as instituições funcionam de acordo com seu próprio interesse e preservação. No livre mercado, o interesse próprio de um negócio é servir a seus clientes para lucrar e evitar perdê-los para seus competidores. Esse é um poderoso incentivo para estabelecer uma sólida reputação e manter a clientela satisfeita. O governo e suas terceiras partes monopolistas não possuem incentivo similar ou restrição porque as pessoas precisam lidar com elas. O estado regula todos os aspectos do mundo financeiro, por exemplo, o que força todos aqueles que desejam bancar ou negociar a interagir com instituições reguladas pelo estado.

Não há competição para a qual os monopólios possam perder clientes, e os monopólios que atendem necessidades humanas básicas nunca irão carecer de enchentes de clientela coagida. Se alguém precisa de uma conta bancária ou de um cartão de crédito para funcionar, então ele precisa aceitar quaisquer termos de serviço que o sistema bancário requer. Não há dúvida que esses termos beneficiam o banco e não o consumidor.

Aqueles que trabalham para terceiros estatistas não são necessariamente pessoas más, mas suas intenções e caráter não importam para o resultado. Burocratas, serventes civis, e banqueiros podem verdadeiramente acreditar que sua obra promove o bem público. Eles podem estar bem sorridentes, estar conscientes no trabalho, e até serem prestativos àqueles que usam seus serviços. Mas, isso não influencia o conteúdo do que eles produzem, a saber: um monopólio mandatado, através do qual o estado controla a riqueza e o comportamento da sociedade. Um burocrata bem-intencionado é parecido com um homem que trabalha em uma fábrica de conservas de atum e anuncia um dia que ele quer fabricar doces em vez de peixe enlatado. Na medida em que ele segue as regras da fábrica e usa as máquinas, ele irá produzir latas de atum e não barras de chocolate. Suas intenções não importam porque é o maquinário e o protocolo da fábrica o que determina o produto. O mesmo é verdade para agências do estado. Um policial pode sinceramente anunciar sua intenção de proteger direitos individuais contra a agressão do estado, mas enquanto ele segue as regras e mecanismos da imposição da lei, o produto resultante irá violar direitos individuais e sustentar o estado. Esse é um ponto importante do porquê um ataque ao estado não deveria se tornar um ataque a seres humanos que poderiam se tornar colegas viajantes.

O dilema: o comércio moderno e as finanças internacionais requerem intermediários, tal como um sistema de bancos interconectados que transmite dinheiro por uma longa distância. Novamente, a necessidade das pessoas por comércio as deixa abertas para exploração e controle pelo estado que apropria riqueza e informação ao dominar os intermediários.

Satoshi elegantemente resolveu esse problema. A cripto permite que as pessoas transfiram riqueza em uma base peer-to-peer que não requer intermediário, nenhuma terceira parte confiável. As transferências não podem ser arbitrariamente revertidas ou alteradas, de modo que

as duas partes não precisam confiar ou conhecer um ao outro; as intenções são irrelevantes. O melhor aspecto do escambo é mantido – troca direta – enquanto os piores aspectos caem por água abaixo – barreiras geográficas e uma limitada diversidade de bens. Visto que pessoas podem manter suas próprias carteiras, a necessidade de recorrer a um estabelecimento de armazenamento ou agente de transferência é também eliminada. Cada usuário pode funcionar como um banqueiro de si mesmo com carteiras seguradas por chaves privadas que previnem olhos e dedos maliciosos.

As implicações para a liberdade individual são profundas.

A Necessidade de um Dinheiro Descentralizado

Para as pessoas comuns se elevarem para além do escambo e abraçar a prosperidade do comércio moderno, um meio de troca é necessário – isto é, uma moeda corrente é necessária.

Economistas escrutinizam as características que um meio de troca desejável possui, tais como a ampla aceitação, durabilidade e fungibilidade.

Mas um aspecto crucial de uma moeda sólida é frequentemente ignorado: quem controla ela? Quem emite a moeda e decide as regras pelas quais ela circula? Uma moeda é tão sólida quanto as regras dentro das quais ela joga. Nos fins extremos do continuum social, há duas possíveis respostas. A moeda corrente está sob controle centralizado de uma autoridade ou o sob o controle descentralizado de cada pessoa a usando. Em outras palavras, a moeda corrente ou expressa o poder do estado ou a liberdade do indivíduo.

Em uma sociedade primitiva, a questão do que constitui uma moeda corrente válida é determinada pelas pessoas que negociam; elas podem decidir que querem usar conchas do mar, por exemplo. Para um observador de fora, a dinâmica poderia se assemelhar a um consenso centralizado porque a maioria das pessoas iriam achar conveniente escolher a mesma moeda corrente e tolerar as mesmas regras evoluídas. A moeda corrente, na verdade, expressa descentralização porque todo indivíduo pode resgatar sua participação a qualquer tempo e oferecer outros meios de troca. Essa é a característica definidora da descentralização; o indivíduo livremente entrega ou retira seu consentimento.

É dito que a sociedade moderna precisa de centralização porque sua complexidade requer coordenação massiva. Sociedades avançadas,

argumenta-se, demandam que decisões sejam coordenadas por um governo que crie a moeda corrente, defina sua circulação e elimine a fraude. Desconsiderando a objeção moral contra um monopólio da moeda corrente – a saber, que é errado compelir indivíduos pacíficos a usar ou a fazer qualquer coisa – ao menos duas outras objeções existem. A primeira fora esboçada anteriormente. O governo e suas instituições aliadas agem em prol de seu próprio enriquecimento e preservação, não em prol do interesse dos indivíduos forçados a usarem seus "serviços".

A segunda objeção é utilitária. Em sua Aula Memorial do Nobel de 1974, "The Pretense of Knowledge", o economista liberal clássico Friedrich Hayek explica:

> O reconhecimento dos limites insuperáveis para esse conhecimento deve […] ensinar ao estudante da sociedade uma lição de humildade a qual deveria protegê-lo de se tornar um cúmplice da batalha fatal do homem para controlar a sociedade – uma batalha que não apenas o fará um tirano sobre seus semelhantes, mas que pode muito bem fazê-lo o destruidor de uma civilização ao qual nenhum cérebro designou, mas sim que cresceu dos esforços livres de milhões de indivíduos.

Ninguém possui informação o suficiente sobre as bilhões de transações que acontecem a todo minuto para centralizar ou controlá-las. Mesmo se fosse possível fazer isso por um momento congelado no tempo, o que não é o caso, preferências humanas e suas circunstâncias são imprevisíveis e talvez mudassem no próximo momento. O que foi verdade ontem pode não ser verdade hoje. Em resumo, Hayek acreditou que a engenharia social aleijou, ao invés de ter criado, a sociedade, porque ela impôs ignorância e preveniu os indivíduos de agirem segundo seu próprio interesse. Uma sociedade saudável é o resultado da ação humana, mas não do desígnio humano.

Um argumento pela centralização imediatamente surge. Se todo indivíduo persegue seu próprio auto interesse, então o caos é dito ser o resultado inevitável, especialmente quando um empenho envolve muitos indivíduos. O oposto é verdadeiro. O filósofo inglês do século XIX Herbert Spencer argumenta persuasivamente contra a noção de que a ordem social foi manufaturada pela coordenação através da lei. Em vez

disso, ele acreditava que a ordem desabrocha naturalmente das “cooperações espontâneas do homem perseguindo seus interesses privados.”

Spencer contrasta duas formas de ordem: fileiras de soldados marchando em tandem (sociedade militar) e ordem espontânea (sociedade industrial). A última pode assemelhar-se ao caos, mas é na verdade uma forma inigualável de coordenação. Considere uma grande loja de departamentos durante uma corrida de Natal ao shopping. Uma pessoa olhando de cima a cena de uma perspectiva semelhante a divina veria as pessoas correndo em diferentes direções, às vezes esbarrando umas nas outras ou parecendo perdidas. Vendedores pegam itens do estoque apenas para colocá-los no chão de novo antes de se dispararem em diferentes direções. Eles desdobram roupas apenas para deixá-las em uma pilha bamba. O anúncio de uma promoção relâmpago faz com que elas entrem em uma debandada rumo à pechincha. Funcionários da loja correm de um lado para o outro para responder perguntas ou para dar desconto às pessoas. A cena pareceria “anarquista” no sentido caótico da palavra.

O que o observador vê, entretanto, é uma sofisticada versão da ordem espontânea pela qual todas as partes pacificamente atingem seus próprios caminhos sem coordenação centralizada. É um microcosmo do livre mercado em funcionamento. A loja quer vender seus bens, os empregados querem manter seus trabalhos, os clientes querem presentes. O que parece ser uma correria de várias formigas é o comportamento consciente e orientado a fins de indivíduos que não-intencionalmente beneficiam uns aos outros enquanto satisfazem suas próprias necessidades. Sem compradores no Natal, a loja pode ir à falência, os balconistas perderiam seus empregos; os vendedores não teriam pacotes embaixo da árvore de Natal. O caos aparente é o livre mercado trabalhando para satisfazer as necessidades das pessoas sem planejamento central, sem coordenação. E todos estão satisfeitos.

A Dinâmica da Cripto é similar. Sua descentralização de livre mercado depende de um consenso a partir do qual todos são livres para retirar seu consentimento sem punição. Os participantes não requerem conhecimento de transações além da deles mesmos, e eles chegam na blockchain de todas as direções para diferentes propósitos. O que parece caos é na verdade uma sofisticada forma de ordem que beneficia a todos.

O Primado da Privacidade

A privacidade da cripto é imperfeita, embora melhorias tecnológicas estejam sendo feitas. Ela providencia pseudonimato – um estado de identidade discreta que permite a confirmação de um usuário sem revelar sua identidade legal. Ademais, a cripto oferece uma forte camada de proteção contra abusos do estado e outras ameaças que surgem de olhos intrusivos. Instrumentos como os mixers podem, além disso, aumentar a proteção das criptos da identidade das pessoas, de seu Nome Verdadeiro. (Mais será dito sobre esse conceito.)

Privacidade e liberdade estão intimamente ligadas. Imagine um mundo onde a renda não é registrada. Como iriam os impostos ser coletados ou contas de banco confiscadas quando o governo não sabe o que você tem ou onde você tem? Se o registro de eventos de vida como o nascimento ou o ingresso na escola são privados, como poderiam nossas crianças serem recrutadas? Se a permissão não é requerida para abrir um negócio, como poderiam as regulações serem impostas? O maquinário do governo é paralisado sem a informação sobre quem você é e o que você tem. É por isso que seu apetite por dados é voraz. Conhecimento é poder. (Nota: as palavras "governo" e "o estado" estão sendo usadas intercambiavelmente).

Emprego, finanças, histórico médico, elegibilidade militar, educação, residência, estado conjugal, registro de telefone, hábitos de viagem, uso de internet, propriedade de automóveis e uma miríade de outros dados são ou armazenados pelo governo ou facilmente acessados por ele. A cripto providencia um raro oásis de privacidade baseado em algoritmos e pseudonimato. Quando a carteira de alguém envia um pagamento a outra, a chave daquele que enviou é decodificada pela chave de quem recebeu. A encriptação protege a transação de intromissão ou roubo. Sua privacidade protege a vida das pessoas do estado.

Essa é a visão de Satoshi Nakamoto: um sistema de comércio peer-to-peer, descentralizado e pseudonímico de comércio e de serviços bancários próprios através do qual o indivíduo evita a corrupção do atual sistema ao evitar utilizar terceiras partes confiáveis. Indivíduos privatizam as suas próprias vidas. Depois da prensa de Gutemberg, poucas invenções criaram tanta libertação e oportunidades para a liberdade.

Isso permanecerá verdade, entretanto, apenas se a visão original for sustentada e não comprometida por aqueles que perseguem "respeitabilidade" e equalizam essa palavra com sanção do estado.

Conclusão

A introdução focou na contribuição das criptos para o poder e para a liberdade dos indivíduos, mas o benefício da cripto para a sociedade civil é imenso.

Talvez nenhum outro autor tenha sido melhor em capturar os benéficos do auto interesse descoordenado da sociedade do que o filósofo do Iluminismo Francês François-Marie Arouet de Voltaire.

Em suas *Cartas a respeito da Nação Inglesa*, Voltaire pergunta o porquê de haver tanta tolerância religiosa na Inglaterra em comparação com a França, a qual foi despedaçada por conflitos brutais entre católicos e protestantes. Não foi devido a leis ou a história. As leis britânicas favoreciam fortemente a Igreja da Inglaterra e a perseguição passada foi severa o suficiente para fazer com que os Peregrinos fizessem uma perigosa viagem para um Novo Mundo. A diferença chave entre a Inglaterra e a França, conclui Voltaire, era a rede de comércio relativamente livre pela qual as pessoas comuns lidam umas com as outras somente por auto interesse financeiro. A diferença foi o surgimento de uma classe média comercial que rendeu para a Inglaterra o apelido de "uma nação de vendedores". A liberdade financeira alimentou a tolerância e a civilidade da sociedade.

Voltaire declara:

> Vá para a Bolsa de Londres, aquele lugar mais venerável que muitos tribunais, e você verá representantes de todas as nações reunidos lá em prol do lucro da humanidade. Lá o judeu, o maometano e o cristão lidam um com o outro como se fossem da mesma religião e reservam o nome de infiel para aqueles que vão a falência. Lá o presbiteriano confia no anabatista, e o anglicano aceita a promessa do quaker. Ao sair dessas reuniões pacíficas e livres, alguns vão à sinagoga, outros em busca de bebida; outro homem está a caminho de ser batizado em uma grande banheira em nome do Pai, pelo Filho, ao Espírito Santo; aquele homem está vendo o prepúcio de seu filho ser cortado, e uma fórmula hebraica será murmurada sobre a criança da qual ele mesmo não entende nada; alguns outros estão indo para sua igreja

> esperar a inspiração de Deus com seus chapéus; e todos estão satisfeitos.

Ao permitir o livre fluxo de comércio e de riqueza, a cripto enriquece não apenas os indivíduos, mas também a sociedade civil, porque a interação financeira é a base da tolerância. Ela quebra barreiras raciais, étnicas e de classe. Bem como uma sociedade de encorajamento saudável, a cripto oferece diversidade de escolha para o indivíduo. Alguns usuários irão escolher o anonimato, enquanto outros podem divulgar suas identidades. Alguns irão ser individualistas severos e anarcocapitalistas, enquanto outros podem preferir o socialismo. Diferenças de ideologia, religião ou estilo de vida são irrelevantes para as transações em blockchain porque elas são cegas a tais delicadezas. Elas reconhecem apenas o consenso.

Uma sociedade em prosperidade é uma na qual as pessoas se reúnem em prol de seu próprio lucro, seja o lucro definido em termos monetários ou em termos culturais. Eles se reúnem em independência e liberdade. Eles separam seus caminhos quando querem seguir em frente. E todos estão satisfeitos.

SEÇÃO UM

O Problema da Terceira Parte Confiável

C A P Í T U L O U M

Ouvindo o Passado

> "O problema chave com as moedas correntes convencionais é toda a confiança exigida para fazê-la funcionar. O banco central precisa ser confiado para que não venha a degradar a moeda corrente, mas a história das moedas fiduciárias está cheia de violações dessa confiança. Os bancos devem ser confiados para manter o nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito mesmo que mal tenham uma fração de reserva. Temos de confiar a eles a nossa privacidade, confiar neles para que não deixem ladrões de identidade drenarem nossas contas."
> – Satoshi Nakamoto

O problema das terceiras partes confiáveis têm assombrado os sistemas financeiros modernos e corretoras centralizadas porque as pessoas requerem um intermediário para fazê-las funcionar. Os bons ou maus motivos da terceira parte se tornam um aspecto definidor da transação, e aqueles que usam as instituições estão à mercê dessas intenções. Isso é especialmente verdade para o atual sistema de moeda emitida pelo estado e para o sistema bancário central.

Um sistema sem necessidade de confiança evita intermediários e não depende das intenções dos participantes; isto é, o sistema funciona da mesma maneira independente da intenção de qualquer parte. A blockchain, com um protocolo peer-to-peer imutável e transparente, é chamada de isenta da necessidade de confiança, porque não há intermediário corruptível do qual as trocas precisam depender.

Em uma pequena escala, o problema das terceiras partes confiáveis precisa sempre existir porque um intermediário é útil ou necessário em algumas situações. Se terceiras partes confiáveis oferecem serviços competitivos num livre mercado, entretanto, o dano da desonestidade ou incompetência é limitado. As pessoas podem levar seus negócios a todos os lugares, reportar um vigarista aos guardas, advertir aos outros e mover uma ação judicial.

Um terceiro ocasionalmente desonesto não é o problema, Satoshi adverte. Ele fala sobre a corrupção institucionalizada do governo e dos

bancos centrais a partir dos quais a pessoa comum não poderia escapar usando um competidor ou por processo judicial. Quase todos que trabalham numa mesa, dirigem um negócio, compram ou vendem bens, aceitam benefícios do governo ou pagam impostos tiveram de aceitar uma moeda fiduciária que constantemente afunda em termos de valor devido à inflação. Quase todos que usam crédito, aceitam cheques, tomam empréstimos, conduzem comércio ou fazem negócios no exterior precisam passar por bancos que roubam como assaltantes bêbados.

Para as pessoas comuns, a situação costumava parecer desesperançosa porque nenhuma alternativa legal, prática e privada existia para transferir fundos por consideráveis distâncias, incluindo fronteiras. Tentativas de reformar ou remover o sistema também pareciam condenadas porque elas eram inerentemente corruptas e auto servientes. De fato, o serviço bancário central e a moeda fiduciária estavam servindo ao propósito para o qual eles foram estabelecidos: controle financeiro pelas elites. A necessidade das pessoas por dinheiro e trocas se tornaram suas camisas de força.

E então veio Satoshi. E então vieram a blockchain e a cripto. Um novo conceito de dinheiro foi criado de uma forma que não pode ser inflacionada; o número de bitcoins é fixo em 21 milhões de unidades divisíveis. A oferta pode apenas diminuir quando moedas são perdidas, como inevitavelmente ocorre. Satoshi nota, "Moedas perdidas apenas fazem as moedas de todos os outros valerem um pouco mais. Pense nisso como se fosse uma doação a todos." O Bitcoin resolveu o problema da moeda fiduciária.

Um novo conceito de transferência financeira resolveu o problema das terceiras partes confiáveis, especialmente no que diz respeito aos bancos. Embora transações peer-to-peer envolvam um intermediário ou minerador, nenhuma confiança é requerida visto que a transação é lançada apenas quando a "proof of work" é feita, o que consiste em resolver um complicado problema matemático. Chegar numa solução pode ser custoso do ponto de vista do poder computacional e gasto de tempo, mas as soluções em si mesmas são fáceis de verificar. Satoshi comenta, "Com uma moeda eletrônica baseada em prova criptográfica, sem a necessidade de se confiar numa terceira parte intermediária, o dinheiro pode se tornar seguro e as transações tornadas fáceis." A solidez e propriedade do protocolo da blockchain é assegurada pelo uso de opensource que é visível a todos e por todos verificável. O resultado

político: Uma moeda corrente privada e um método de troca que libertou as pessoas da opressão financeira.

A própria ideia de uma moeda privada é, entretanto, dificilmente nova.

Precedentes na Teoria Individualista Radical

O velho Friedrich Hayek é o economista austríaco mais respeitado do século XX. Seu livro *The Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies* argumenta vigorosamente a favor de moedas correntes privadas e competitivas, para que substituam as moedas emitidas pelo governo. Hayek pondera uma questão chave. "Quando se estuda a história da moeda não será de ajuda perguntar o porquê de as pessoas terem persistido com governantes exercendo um poder exclusivo por mais de dois mil anos que foram regularmente usados para explorar e defraudá-las. Isso pode ser explicado somente pelo mito" de que a moeda do governo precisava "tornar-se tão firmemente estabelecida que não passou pela cabeça dos estudantes profissionais dessas áreas [...] sequer questionar isso. Mas uma vez que a validade da doutrina é questionada, seu fundamento é rapidamente percebido como frágil."

Os governos arrancam lucros incríveis ao degradar a moeda, mas o jogo manipulado funciona apenas se as pessoas não têm alternativa senão jogá-lo. O propósito político das leis bancárias e de curso forçado é garantir um monopólio ao estado, que permitem a redistribuição de riqueza e de poder das pessoas comuns para além da elite da sociedade. A moeda fiduciária e os sistemas bancários, entretanto, permanecem frágeis, porque o sistema depende de pessoas que ou não entendem as dinâmicas, ou que entendem e não tem escolha. Hayek se pergunta o porquê de o entendimento público ser tão enganoso. Pois havia "um monopólio do governo da provisão de dinheiro [...] universalmente tido como indispensável" e o que iria acontecer "se a provisão do dinheiro fosse aberta para a competição de preocupações privadas ofertando diferentes moedas correntes?"

Com estranha presciência, Hayek argumenta a favor de moedas correntes desenvolvidas por empreendedores que inovam em novas formas de dinheiro assim como eles inovam em outras áreas. Uma das desvantagens do monopólio do governo é que ele impõe um congelamento do tipo de invenções que agora correm livres nas criptos. O historiador

voluntarista Carl Watner observa: “Ninguém pode falar em antecipação quais as formas de moedas que podem surgir porque ninguém tem certeza de que escolhas os indivíduos fariam ou que novas tecnologias podem ser descobertas. Leis forçando as pessoas a usarem o dinheiro do Federal Reserve System congelaram os desenvolvimentos monetários em um certo estágio. […] Imagine se o Congresso tivesse protegido os Correios ao aprovar leis que iriam ter prevenido as pessoas de se comunicar via internet. Nós nunca iríamos ter experienciado as maravilhas do e-mail.”

O tardio economista austríaco Murray Rothbard também disputa a questão de “por que as pessoas resistem tão vigorosamente a moedas privadas?” Em seu livro *For a New Liberty: The Libertarian Manifesto* ele antecipa uma explicação." Se o governo e apenas o governo tivesse tido um monopólio da manufatura de sapatos e dos negócios de varejo, como iria a maior parte do público tratar o libertário que veio agora defender que o governo saia do negócio de sapatos e que o mercado seja aberto para os empreendimentos privados?". Rothbard prevê que os céticos iriam atacar o libertário por privá-lo da única fonte possível de sapatos – o governo. As pessoas são completamente doutrinadas a acreditar que a vida cotidiana não pode funcionar sem o estado e a moeda fiduciária.

Hayek e Rothbard são incomuns entre os economistas do livre mercado no que diz respeito a sua adoção ao dinheiro e a sistemas monetários privados. Até mesmo os zelotes do laissez-faire raramente defendem moedas de livre mercado ou serviços bancários privados. Em vez disso, eles debatem questões marginais tais como reserva fracionária e outras reformas que eles acham que irão melhorar o sistema existente. Ou eles argumentam pela restauração de um padrão ouro como se isso fosse uma panaceia. Mas, se um padrão ouro fosse aplicado à moeda fiduciária, o sistema ainda iria exigir que as pessoas confiassem no governo e nos bancos. Isso significa confiar que ambas as instituições iriam agir contra os seus próprios interesses, os quais eles historicamente negligenciaram-se a fazer.

A negligência moderna do dinheiro e dos serviços bancários de livre mercado é estranha porque os individualistas do século XIX focaram intensamente na importância da moeda privada e dos serviços bancários privados para a libertação pessoal. Eles colocaram uma ênfase primária no direito de todo indivíduo criar a sua própria moeda e funcionar como o seu próprio banco. Era um direito natural tão importante

quanto a liberdade de fala ou religião. O proeminente individualista Benjamin Tucker acreditou que o direito de usar a moeda privada era tão importante que esse direito poderia destruir o Estado totalmente por si mesmo. Seu raciocínio: o monopólio monetário, incluindo o controle do crédito, foi como o Estado sustentou a si mesmo e roubou as pessoas comuns não apenas de riqueza, mas também de oportunidades econômicas.

Dois eventos específicos esculpiram a abordagem que os primeiros anarquistas individualistas adotaram em relação ao monopólio monetário. Um deles foi o *Pânico de 1837*, que levou os Estados Unidos à recessão até meados da década de 1840. As causas comumente citadas do Pânico incluem uma bolha imobiliária em colapso e uma queda acentuada nos preços do algodão. A culpa também é colocada nos pés do presidente Andrew Jackson por vetar a recuperação do Segundo Banco dos Estados Unidos e precipitar uma infeliz cadeia de eventos econômicos. Baseando-se no trabalho do professor de economia Peter Temin, Rothbard contesta essa interpretação.

> Primeiro, ele [Temin] aponta que a inflação de preços realmente começou mais cedo, quando os preços em geral atingiram um mínimo de 82% em julho de 1830 e depois subiram em 20,7% em três anos para chegar a 99% no outono de 1833. A razão para o aumento de preço é simples: A oferta total de dinheiro havia aumentado de $109 milhões em 1830 para $159 milhões em 1833, um aumento de 45,9%, ou um aumento anual de 15,3%. Dividindo ainda mais os números, a oferta total de dinheiro aumentou de $109 milhões em 1830 para $155 milhões um ano e meio depois, uma expansão espetacular de 35%. Inquestionavelmente, essa expansão monetária foi estimulada pelo ainda florescente Banco dos Estados Unidos, que aumentou suas notas e depósitos de janeiro de 1830 a janeiro de 1832 de um total de $29 milhões para $42,1 milhões, um aumento de 45,2%. Assim, a inflação de preços e dinheiro nos primeiros anos da década de 1830 foi novamente desencadeada pela expansão do ainda dominante banco central.

Pode-se dizer que o Pânico começou em maio de 1837, quando os bancos da cidade de Nova York anunciaram que não iriam resgatar

papel comercial em espécie pelo valor de face integral. Dos aproximadamente 800 bancos nos Estados Unidos, todos, exceto seis, pararam em um ponto ou outro de resgatar notas e depósitos por moedas de ouro ou prata. A suspeita e o ódio aos bancos tradicionais e ao dinheiro emitido pelo governo dispararam, com radicais examinando sistemas alternativos.

O outro evento que impactou dramaticamente a febre radical da reforma monetária foi a Guerra Civil, pela qual o Norte financiou sua luta por meio de Leis de Curso Legal e do National Banking Act de 1863.

Os radicais não apenas teorizaram; eles experimentaram moedas privadas e novos modelos econômicos. Seus esforços são fascinantes, mas também são histórias de advertência. Um grande problema para o anarquismo individualista do século XIX foi a aceitação geral do movimento de que havia um elo entre dinheiro sólido e a teoria do valor-trabalho. Esta teoria afirma que o verdadeiro valor de um bem ou serviço é baseado no trabalho necessário para produzi-lo, e não no preço pelo qual um vendedor e um comprador estão dispostos a trocar. Em suma, um bem tem valor intrínseco e não subjetivo. (Mais sobre isso na seção sobre o Teorema da Regressão). Felizmente, seu principal objetivo econômico era a abolição do "monopólio do dinheiro". O termo se referia a três formas diferentes, mas interativas de monopólio: bancos, cobrança de juros e emissão privilegiada de moeda. A abolição do poder estatal sobre a moeda era o foco, e eles evitavam o uso da força para implementar seus próprios esquemas.

Josiah Warren forneceu um exemplo real do que se entende por moeda baseada na teoria do valor-trabalho. Creditado como o primeiro anarquista americano, Warren testou sua solução específica para o monopólio do dinheiro através de uma Loja de Tempo da qual ele emitiu "Notas de Trabalho". Em 1827, a empresa abriu com $300 em mantimentos e produtos secos que foram oferecidos com uma margem de 7% dos custos de Warren para cobrir despesas de administração. Isso foi antes de os mantimentos serem pré-embalados ou pré-pesados, e era comum que os compradores negociassem com o lojista em vez de pagar um preço postado. Uma das inovações de Warren foi colocar preços, o que reduziu os custos porque as transações consumiam menos tempo. O cliente pagou em dinheiro tradicional pelas mercadorias e pagou com uma Nota de Trabalho para compensar Warren por seu tempo. A Nota de Trabalho obrigava o cliente a fornecer a Warren uma quantidade

equivalente de seu tempo. Se a compradora fosse uma costureira, por exemplo, a Nota de Trabalho a obrigava a render a Warren X unidades de tempo para produzir roupas. O objetivo de Warren era estabelecer uma economia – ou pelo menos estabelecer uma prova de princípio – na qual o lucro fosse baseado na troca de tempo e trabalho. As Notas de Trabalho circularam e foram amplamente negociadas na comunidade.

Até certo ponto, Warren teve sucesso. As pessoas viajavam centenas de quilômetros de distância para aproveitar os preços baixos da Loja de Tempo. Depois de alguns anos, ele declarou o experimento um sucesso e fechou a loja. Que as Notas de Trabalho tenham sido um sucesso é questionável, no entanto. A própria loja pode ter tido sucesso devido aos seus preços baixos, não às Notas. Qualquer que seja a explicação verdadeira, é difícil ver como essa nova moeda poderia funcionar em populações densas ou em uma escala maior de comércio. Poucas pessoas hoje estariam convencidas da viabilidade do dinheiro privado com base no experimento da Loja de Tempo.

O que será que convenceria o público e os economistas de que as moedas privadas funcionam tão bem ou melhor do que as emitidas pelo governo? Voltar um pouco mais longe na história americana é um bom ponto de partida, porque o futuro sempre se sustenta no passado.

A América nasceu na moeda privada

A América colonial ensina lições poderosas sobre moedas privadas.

As colônias britânicas naturalmente usavam moeda britânica, mas as políticas monetárias duvidosas da pátria também criaram um apetite voraz por dinheiro alternativo. Rothbard explica em *A History of Money and Banking in the United States: The Colonial Era to World War II*, “A Grã-Bretanha estava oficialmente em um padrão de prata […] No entanto, a Grã-Bretanha também cunhou ouro e manteve um padrão bimetálico. […] Na Grã-Bretanha dos séculos XVII e XVIII, o governo manteve uma razão de cunhagem entre ouro e prata que consistentemente supervalorizou o ouro e subvalorizou a prata em relação aos preços do mercado mundial.” As políticas da Grã-Bretanha criaram um mercado robusto de substitutos para seu próprio dinheiro.

A Lei de Gresham governava o dinheiro colonial da mesma forma que governa todas as moedas. A Lei: se duas moedas forem oficialmente avaliadas pelo mesmo preço ou por uma proporção fixa e o valor

de mercado de uma for maior, então a moeda mais valiosa desaparecerá da circulação geral e será usada de outra maneira, como a acumulação de poupança ou pagamento de dívidas externas. Este é o significado do axioma "a moeda ruim expulsa a boa". Moedas de prata encorpadas começaram a desaparecer da circulação dentro das colônias, se transformaram em prata mais leve, dinheiro baseado em mercadorias ou moedas estrangeiras e cunhadas de forma privada. Essas moedas funcionavam como moedas totalmente paralelas, com os peso de ocho espanhóis sendo particularmente populares.

A primeira moeda americana cunhada em particular parece ser o Granby ou Higley Token, que foi cunhado por Dr. Samuel Higley de Connecticut em 1737. Após a morte de Samuel, seu irmão John produziu as moedas de cobre de 1737 a 1739 inclusive. Avaliando as fichas em três pence cada, John supostamente gastou a maioria delas no bar local, até que o barman se recusou a aceitar mais. Em seguida, ele lançou moedas com um lado dizendo "Valore-me como quiser" e o outro lado declarando "Eu sou bom cobre". Nenhum valor foi estampado na moeda, o que era prática comum naqueles dias. Eles circularam amplamente por muitos anos, mesmo depois que John deixou de os cunhar, porque eram uma liga confiável com a qual os ourives faziam joias. Análises metalúrgicas posteriores do Granby descobriram que as moedas eram 98-99% de cobre puro.

Outra lição: o ourives de Nova York do século XVIII, Ephraim Brasher, demonstrou um método pelo qual as moedas cunhadas em particular podiam circular amplamente e sem dúvidas sobre sua pureza ou peso. Muitos cunhadores privados tinham boa reputação dentro de suas próprias comunidades, mas a circulação de suas moedas era frequentemente limitada a esses arredores. Brasher ofereceu uma solução. Ele tornou-se conhecido por testar moedas nas quais carimbava "EB" se provassem ser seguras. Apoiadas por sua reputação, as moedas carimbadas migraram por toda parte.

Esta é uma grande vantagem que a cripto tem sobre as moedas privadas anteriores; suas moedas não têm a mesma necessidade de serem lastreadas por verificação. Ao contrário das moedas físicas, as bitcoins não podem ser raspadas, falsificadas, diluídas por ligas ou negadas pelos maus atos dos mineradores ou dos usuários. Um bitcoin é um bitcoin, e ninguém pode alterar esse fato. Isso evita a verificação de pureza ou peso.

Como e por que o governo proibiu o dinheiro privado

Como a ratificação da Constituição dos Estados Unidos em 1788 afetou o dinheiro privado?

Pessoas assumem que a Constituição dos Estados Unidos concede ao Congresso um "direito" de monopólio de emitir dinheiro. A suposição vem do artigo 1º, Seção 8, Cláusula 5 da Constituição que delega ao Congresso o poder de "cunhar moeda, regular seu valor, e de moeda estrangeira, e fixar o padrão de pesos e medidas". Este é considerado um direito de monopólio. Em seu panfleto "A Inconstitucionalidade das Leis do Congresso Proibindo Correios Particulares" (1844), o jurista e defensor do dinheiro privado Lysander Spooner explica o contrário:

> [Os] poderes do Congresso [...] para "cunhar dinheiro" são na realidade exclusivos apenas contra os governos de outros estados. [...] A proibição constitucional sobre os indivíduos de cunhar dinheiro não se estende além das proibições de "falsificar os títulos e moedas atuais dos Estados Unidos". Desde que os indivíduos não "falsifiquem" ou imitem "os títulos ou moedas correntes dos Estados Unidos", eles têm todo o direito, e o Congresso não tem poder para proibi-los de pesar e analisar peças de ouro e prata, marcar neles seus pesos e pureza e vendê-los pelo que eles trouxerem em competição com a moeda dos Estados Unidos.

A Constituição trata da regulamentação da "moeda estrangeira", mas as moedas domésticas privadas permaneceram populares, especialmente uma chamada de Bechtler.

O século XIX viu uma onda de corridas de ouro na América do Norte. No final da década de 1820, tanto a Geórgia quanto a Carolina do Norte experimentaram grandes corridas e um dilema que as acompanhava. Não havia cunhagem governamental na área. O envio de ouro para a principal casa da moeda na Filadélfia era problemático, porque custava muito para transportar e segurar. Um jornal local explicou a situação da mineradora:

> Já que o Banco do Estado limitou suas emissões e está recolhendo em seus cofres as notas que foram emprestadas

> aos nossos cidadãos, na liquidação de suas contas pendentes, grande inconveniência tem sido deixada em transações comerciais com o Banco, e para fins comuns de comércio. Até que ponto esse esquema [ter uma casa da moeda privada] conseguirá concretizar esses objetos, ainda temos que aprender. O risco e a despesa de enviar ouro para a casa da moeda [Filadélfia] é tal que os proprietários das minas muitas vezes acham difícil descartar os produtos das minas a um valor justo, como as coisas estão agora. Tendo falhado a petição urgente ao Congresso para o estabelecimento de uma filial da Casa da Moeda dos EUA na "região do ouro", e o ouro produzido estando em condições justas de desaparecer completamente do país e cair nos tesouros enferrujados da Europa, esse esquema foi utilizado.

Os garimpeiros procuraram o respeitado relojoeiro e ourives Sr. Christopher Bechtler para uma solução particular. Por ser também metalúrgico e homem honesto, Bechtler era o candidato perfeito para começar a cunhar moedas. A primeira moeda de ouro Bechtler emitida em 1831 foi seguida de anúncios declarando que Bechtler cunharia o ouro de qualquer minerador por 2,5% do ouro.

A reação do governo à competição pode ser julgada pelo fato de que o Tesouro dos Estados Unidos perdeu pouco tempo testando as novas moedas, provavelmente na esperança de desacreditá-las. Infelizmente para o Tesouro, os Bechtlers eram mais puros do que as emissões governamentais. De fato, a Casa da Moeda Federal comprou $294.000 em Bechtlers e os usou para pagar dívidas e negociar com a Europa. De repente, o governo foi motivado a abrir sua própria casa da moeda federal em Charlotte, Carolina do Norte, que ficava a cerca de 130 quilômetros da de Bechtler. A Casa da Moeda Federal começou a produzir moedas de ouro em 1838.

Na época da morte do Sr. Bechtler, consideravelmente mais de um milhão de Bechtlers circulavam amplamente na América, particularmente no Sudeste. A partir daí, porém, os parentes que assumiram o negócio eram incompetentes ou desonestos. A consistência e a pureza diminuíram, e o mercado respondeu se afastando. A casa da moeda fechou alguns anos depois porque ela viveu e morreu de sua reputação.

Os Bechtlers originais continuaram a circular, no entanto. Eles eram tão populares que, durante a Guerra Civil Americana (1861-1865),

as obrigações monetárias da Confederação foram especificadas como sendo pagáveis em ouro Bechtler, não confederado ou outra moeda emitida pelo governo.

A moeda Bechtler é tanto um conto inspirador quanto um aviso. Ele fala das consequências de integridade e degradação do livre mercado, que não são problemas para a cripto porque são isentas da necessidade de confiança e as moedas não podem ser alteradas. A história de Bechtler também demonstra como o livre mercado supera o governo em termos de mover-se rapidamente para um nicho vazio e produzir qualidade. Como fazem hoje, as moedas de livre mercado superam as emissões governamentais. Se eles deixarem de fazê-lo, a moeda falha devido à Lei de Gresham. Como fez no passado, o governo hoje usa moedas privadas, como ouro e criptomoeda, enquanto tenta minar a concorrência que elas representam por meio de suas leis.

A resistência do governo à concorrência não começou nem terminou com os Bechtlers, é claro. Em seu ensaio "Hard Money in the Voluntaryist Tradition", Watner traça o curso de uma casa da moeda em São Francisco durante a corrida do ouro na Califórnia: Moffat & Co. "A Moffat & Co. foi aparentemente a mais responsável das empresas privadas de cunhagem de dinheiro", pois quando "os negócios de São Francisco colocaram um embargo em todas as cunhagens de moedas de ouro privadas", a exceção foi a Moffat. "O restante das emissões privadas foi logo enviado ao Gabinete de Ensaio dos EUA para ser derretido ou então foi aprovado apenas por seu conteúdo de ouro no comércio."

Inicialmente, a Moffat emitiu lingotes de ouro em concorrência direta com o Gabinete Federal de Ensaio dos EUA porque não existia então nenhum Gabinete de Ensaio do estado. De acordo com o site de referência *Coinfacts*, "o ensaio oficial do governo desses lingotes provou que eles valem mais do que o valor estampado neles". A Moffat superou o governo.

A denominação dos lingotes era muito grande para o comércio normal, no entanto, e os comerciantes exigiam moedas menores. A Moffat havia feito um acordo com o Gabinete de Ensaios dos EUA e agora pedia autoridade para cunhar moedas, bem como os lingotes maiores. Quando a permissão não veio, Moffat começou a cunhar moedas sob sua própria marca e autoridade em 1849. A alta reputação da firma e sua política de resgatar todas as moedas pelo valor nominal fizeram com que sua emissão se tornasse uma moeda circulante popular.

A obstrução do governo não parou com a recusa de autorizar a cunhagem. Em 20 de abril de 1850, o State Assayer, Melter, and Refiner of Gold of California foi estabelecido por lei. Um projeto de lei complementar foi aprovado ao mesmo tempo com o objetivo de frear os cunhadores privados. Junto com uma medida anterior em 8 de abril, o projeto representava um compromisso. *Coinfacts* explicava a posição original que o governo havia tomado em relação a cunhadores como Moffat.

> Foi durante a primeira metade de 1850 que houve uma séria agitação contra a cunhagem privada. O Legislativo da Califórnia considerou um projeto de lei […] que teria rotulado cunhadores privados como falsificadores, e que insistia em sujeitar "os fabricantes ou passadores de tal moeda à penalidade imposta aos cunhadores e falsificadores". O projeto de lei também teria forçado as casas de moeda privadas a resgatar suas moedas em "dinheiro legal". A *Alta Califórnia* imprimiu o projeto de lei junto com um editorial de apoio. O editor apontou ainda a impossibilidade de usar moedas privadas no pagamento da alfândega.

No dia seguinte, a *Alta Califórnia* divulgou uma carta aberta da própria Moffat através da qual ela apelou ao povo de São Francisco. Ela reconheceu que o estado não podia emitir moedas legalmente devido a restrições constitucionais, mas os particulares não tinham restrições semelhantes. Ela apontou para a casa da moeda Bechtler que continuava a produzir moedas, embora o negócio estivesse a apenas 130 quilômetros da filial do governo federal em Charlotte. A Moffat lembrou poderosamente a São Francisco que ninguém jamais havia sido enganado comprando ou aceitando suas moedas.

A primeira lei de compromisso do início de abril proibia a emissão privada de peças de ouro com peso inferior a quatro onças troy. Mais uma vez, este era um tamanho estranho para o comércio normal e quase garantia uma circulação limitada. Por outro lado, o Departamento de Ensaios do estado foi autorizado a fundir lingotes de ouro de duas onças troy. *Coinfacts* observou: "O Escritório Estadual de Ensaios da Califórnia foi uma instituição única na história de nossa nação. Foi a única casa da moeda a operar neste país sob a autoridade de um estado,

depois de 1789. Suas emissões (embora nunca contestadas nos tribunais) podem ter sido ilegais sob a Constituição dos Estados Unidos, que proibia qualquer estado de emitir moedas metálicas ou moedas correntes". O estado usou a artimanha de emitir lingotes que não foram mencionados na Constituição, mas que circulavam como o equivalente a moedas.

O projeto de lei de 20 de abril prejudicou ainda mais os cunhadores privados, exigindo que eles resgatassem suas moedas pelo valor nominal para emissão do governo. Seguiu-se uma complicada ida e volta entre a Moffat e os escritórios de análise estadual e federal. A Moffat recebeu um contrato de cunhagem com o estado e buscou permissão federal para cunhar moedas menores; foi negado. Eventualmente, Moffat voltou a emitir suas próprias moedas em denominações menores, após o governo ter concedido à empresa permissão para emitir moedas oficiais de $10 e $20 para o Gabinete de Ensaio.

O governo federal mudou de tática em 1852. A Alfândega dos EUA de repente se recusou a aceitar os lingotes de US $50 de Moffat, embora tivessem sido emitidos sob a autoridade direta do Gabinete de Ensaios dos EUA.O pagamento da alfândega era o principal uso dos lingotes, mas a lei federal exigia que os impostos fossem pagos em moedas com 900/1000 de pureza, em vez do padrão da Califórnia de 884/ a 887/1000. O Departamento do Tesouro deu o notável passo de se recusar a aceitar moedas emitidas por seu próprio Gabinete de Ensaios. Ela invalidou a sua própria cunhagem.

A história da Moffat & Co. é significativa não apenas porque ilustra como o dinheiro privado pode e irá atender às necessidades públicas, mas também porque revela a determinação absoluta do governo de eliminar a concorrência na moeda e as táticas que costumava usar. As táticas permanecem as mesmas até hoje. Uma é proibir a moeda criminalizando-a, como a legislatura da Califórnia tentou fazer com a acusação de falsificação. Outra é absorver e controlar a concorrência como fez o Gabinete de Ensaio ao contratar com a Moffat. Uma terceira estratégia é colocar enormes obstáculos no caminho das moedas livres, o que equivale a uma proibição de facto e dá uma vantagem decisiva ao dinheiro do governo.

A estratégia do governo funcionou. Watner explica: "Em outubro de 1856, a Casa da Moeda federal aparentemente foi capaz de atender a toda a demanda de moeda em circulação doméstica e para exportação, de modo que as emissões privadas de moedas de ouro desapareceram

silenciosamente. Não há registro de nenhuma outra cunhagem privada na Califórnia depois dessa época.”

A história da cunhagem privada no início da América é profunda, difundida e intimamente ligada ao sucesso econômico da nação. A fraude certamente estava presente, mas a honestidade meticulosa e as soluções para a fraude também. As casas da moeda com grande reputação e bom senso comercial tiveram sucesso, e muitas vezes superaram suas contrapartes governamentais, reduzindo-as ao uso da força (lei) para ganhar vantagem.

O governo não agiu em nome do público. Se tivesse, não teria atacado empresas honestas que prestavam serviços desesperadamente necessários a mineradores, comerciantes e compradores; a necessidade pública de moeda foi ignorada pelo Departamento do Tesouro. A lei também não explica por que alguns governos preferiram usar moedas privadas em algumas ocasiões. Uma explicação faz sentido; o governo queria eliminar a concorrência não porque fosse fraudulenta, mas porque a concorrência poderia vencer em um livre mercado. O governo agiu em seu próprio nome para encher seus bolsos e fortalecer seu poder.

Em 8 de junho de 1864, o Congresso aprovou uma lei para punir e impedir a falsificação de moedas dos Estados Unidos. Dizia, na íntegra:

> Que se qualquer pessoa ou pessoas, exceto as agora autorizadas por lei, fizerem ou fizerem ser feitas, ou emitirem ou passarem, ou tentarem emitir ou passar, quaisquer moedas de ouro ou prata, ou outros metais ou ligas de metal, destinados ao uso e finalidade de dinheiro corrente, seja na semelhança da moeda dos Estados Unidos ou de países estrangeiros, ou de desígnio original, toda pessoa que assim infringir deverá, mediante condenação, ser punido com multa não superior a três mil dólares, ou com prisão por um período não superior a cinco anos, ou ambos, a critério do tribunal, de acordo com o agravamento do delito.

A cunhagem privada de moeda efetivamente cessou na América.

A Lei foi, sem dúvida, vendida ao público como sendo necessária para proteger contra fraudes. Sem desculpar qualquer fraude existente

ou sugerir que o crime não deveria ser punido, uma política de advertência ou "comprador, cuidado" deveria ser aplicada; o comprador é responsável por verificar a qualidade das mercadorias antes de uma compra. Muita fraude poderia ter sido evitada se as pessoas não tivessem confiado nas garantias do governo, mas tivessem aprendido a avaliar a qualidade por si mesmas. Uma categoria inteira e valiosa de negócios foi criminalizada porque alguns participantes eram desonestos e alguns clientes descuidados. Essas foram as desculpas. A principal motivação para o governo foi eliminar a concorrência.

É reputada a Mark Twain a seguinte fala: "A história não se repete, mas rima". Para alguns, a cunhagem privada no início da América pode parecer ter pouco em comum com a cripto, mas há um tema comum. O governo está ameaçado e quer monopolizar ou regular um novo dinheiro privado através de uma mistura de proibição, levantamento de obstáculos, absorção e punição. A história está começando a rimar.

Em última análise, a viabilidade de criptomoedas e outras moedas privadas se resume a duas perguntas: O livre mercado pode fornecer um dinheiro competitivo? E o estado permitirá que o dinheiro privado exista sem regulamentação?

Um grande obstáculo para a aceitação da cripto nos círculos de livre mercado tem sido a convicção de que ela não é e não pode ser um dinheiro válido.

O Teorema da Regressão

O exemplo da moeda de Granby que continuou a circular devido ao seu valor na fabricação de joias ilustra um princípio que gerou debate sobre se a cripto pode ser vista como uma moeda. O conceito é o Teorema da Regressão.

O Teorema da Regressão é uma proposição econômica que está mais associada a Ludwig von Mises. Aplica a teoria subjetiva do valor ao poder de compra ou valor objetivo do dinheiro. O teorema faz isso traçando valores de troca objetivos através da "teoria subjetiva do valor, pela qual os valores são atribuídos aos valores de uso subjetivos finais dos consumidores marginais que valorizam tais bens e serviços por seus valores de uso objetivo que eles esperam consumir". Em outras palavras, o valor de uso objetivo do dinheiro remonta ao ponto em que as pessoas valoravam seus usos não monetários. Isso levanta um problema para a moeda fiduciária que não é consumida como o ouro ou a prata

podem ser. Em vez disso, com a moeda fiduciária, “os valores de uso subjetivo e objetivo do dinheiro coincidem e são iguais ao seu valor objetivo de troca, o valor estimado dos bens e serviços pelos quais ele pode ser trocado.”

O professor de Economia Jeffrey Rogers Hummel descompacta o conceito, revelando como se aplica à moeda fiduciária. O poder de compra do dinheiro de hoje “se baseia no de ontem, e no de ontem desse ontem… e assim em diante. […] Até quão longe a regressão […] vai? Logicamente, Mises explicou, para um dinheiro mercadoria ela vai até o dia em que a mercadoria pela primeira vez passou a ser usada como um meio de troca. Nesse dia, ele teve um valor de troca ou poder de compra devido apenas” a sua importância “como uma mercadoria comum (para consumo ou para uso como uma entrada produtiva) e não para uso como um meio de troca. Pois […] o dólar dos EUA se tornou uma moeda fiduciária ao terminar com a resgatabilidade do que fora uma reivindicação para um dinheiro mercadoria […]. A cadeia histórica regride para o dia antes da terminação, e, portanto, de volta ao dia antes da mercadoria se tornar um meio de troca. A aplicação da lógica para uma nova moeda fiduciária” significa aplicar uma taxa de resgate oficial para uma moeda fiduciária estabelecida.

O teorema tem sido muito influente porque ele elegantemente entrelaça o poder de compra do dinheiro com as teorias de valor subjetivo e de utilidade marginal. A teoria subjetiva do valor argumenta que nenhum bem ou serviço é inerentemente valioso; não tem valor embutido devido ao trabalho necessário para produzi-lo, por exemplo. Em vez disso, seu valor é determinado pela importância do bem ou serviço para os indivíduos específicos que o vendem e consomem. Mas esse valor não permanece constante mesmo para esses indivíduos por causa da utilidade marginal. A utilidade marginal refere-se à satisfação adicional que uma pessoa recebe ao consumir mais uma unidade de um bem ou serviço, medida em números ordinais. Um homem faminto provavelmente valorizaria um prato de comida como o 1° da lista, enquanto uma pessoa com excesso de peso em uma dieta rigorosa pode dar ao mesmo prato uma classificação negativa. Depois de comer o suficiente, o homem faminto provavelmente desvalorizará a utilidade marginal de mais comida e priorizará encontrar abrigo para a noite. Todo valor econômico é subjetivo e está em fluxo.

O Teorema da Regressão precisa ser cuidadosamente ponderado apenas porque muitos economistas austríacos e outros economistas de

livre mercado rejeitam a criptomoeda alegando que ela viola as circunstâncias nas quais o dinheiro válido deve se originar; essas pessoas deveriam ser aliadas naturais da comunidade cripto, não críticas. Enquanto isso, a maioria dos entusiastas de cripto reagem de uma das quatro maneiras ao ouvir a objeção do Teorema da Regressão. Elas não ligam. Assumem a atitude de "se cachorro come, é comida de cachorro"; ou seja, se algo compra bens e serviços, é dinheiro. Eles afirmam que o teorema não se aplica para a era digital. Ou eles insistem que se *aplica* à cripto de uma maneira que é mal compreendida. As duas últimas abordagens são promissoras para resolver o que parece ser uma tensão entre Mises e a cripto. Ambos os lados podem se beneficiar de clarificação.

Um ponto inicial: Um teorema é uma proposição geral que não é evidente em si mesma, mas precisa ser provada por uma cadeia de raciocínios. Tem sido chamado de "uma verdade estabelecida por meio de verdades aceitas". Não é um axioma e é vulnerável a mudanças nas circunstâncias ou no raciocínio adicional. Isso significa que a proposição é maleável.

O economista Robert P. Murphy fornece outro caminho para explicar como o Bitcoin surgiu como um meio de troca sem estar vinculado a uma mercadoria ou resgatável em um valor fixo de uma moeda fiduciária estabelecida. Seu artigo "Why Misesians Need to Tread Cautiously When Disparaging Bitcoin" argumenta: "[As] primeiras pessoas a negociar por ele o fizeram porque lhes fornecia utilidade direta, porque sabiam que havia pelo menos uma chance de servir para irritar os governos do mundo […] [Os] primeiros adeptos do Bitcoin estavam fazendo isso por razões ideológicas, não por razões pecuniárias". Para Murphy, a liberdade é o valor de mercadoria ou serviço do bitcoin.

O cripto-entusiasta Jeffrey A. Tucker usa uma tacada diferente. Em um artigo da *Foundation for Economic Education* intitulado "What Gave Bitcoin Its Value?", ele aponta para o propósito que o teorema serviu originalmente; ajudou a responder à pergunta de por que certas mercadorias surgiram como moedas enquanto outras não. O surgimento do sal como uma moeda, em vez de algas marinhas, foi devido à utilidade direta e durabilidade do sal, por exemplo.

Tucker então liga a cripto não a um bem concreto, mas a um serviço concreto que cumpre com uma necessidade profunda e possui utilidade direta – a saber, a blockchain como um sistema de pagamento.

> Bitcoin é tanto um sistema de pagamento quanto uma moeda. O sistema de pagamento é a fonte de valor [não-monetário], enquanto a unidade de medida expressa esse valor em termos de preço. A unidade de dinheiro e de pagamento é sua característica mais incomum, é aquela que a maioria dos comentadores teve dificuldade em entender […]. Essa lacuna entre dinheiro e pagamento sempre esteve conosco, exceto no caso de proximidade física. Se eu lhe der um dólar por seu pedaço de pizza, não há terceira parte. Mas sistemas de pagamentos, terceiros, e relacionamentos de confiança se tornam necessários uma vez que você deixa a proximidade geográfica. É aí que as companhias como a Visa e instituições como bancos se tornam indispensáveis.

Para Tucker, o valor não-monetário da cripto é um sistema de pagamento que não requer uma terceira parte confiável e não possui limitações geográficas. A blockchain é o que faz a cripto emergir como um meio de troca. Dessa maneira, o Teorema da Regressão é aplicado ao bitcoin, mas o teorema precisa ser atualizado para focar nos serviços únicos – funcionando como bens de facto – que estão disponíveis na era digital.

A última palavra do Teorema da Regressão pertence a Satoshi. Em um post intitulado "Bitcoin does NOT violate Mises' Regression Theorem" no fórum bitcointalk que ele fundou, Satoshi afirma:

> Como um experimento mental, imagine que houvesse um metal base tão escasso quanto o ouro, mas com as seguintes propriedades: – de cor acinzentada – não é um bom condutor de eletricidade – não é particularmente forte, mas também não é dúctil ou facilmente maleável – não é útil para qualquer propósito prático ou ornamental e tem uma propriedade mágica especial: – pode ser transportado através de um canal de comunicação. Se, de alguma forma, adquirisse algum valor por qualquer motivo, qualquer pessoa que quisesse transferir riqueza a longa distância poderia comprá-la, transmiti-la e fazer com que o destinatário a vendesse. Talvez possa obter um valor inicial circularmente como você sugeriu, por pessoas prevendo sua potencial utilidade para

> troca. (Eu definitivamente gostaria de alguns) Talvez colecionadores, qualquer motivo aleatório poderia desencadear isso. Creio que as qualificações tradicionais para dinheiro foram escritas com a suposição de que existem tantos objetos concorrentes no mundo que são escassos, um objeto com o bootstrap automático de valor intrínseco certamente vencerá aqueles sem valor intrínseco. Mas se não houvesse nada no mundo com valor intrínseco que pudesse ser usado como dinheiro, apenas escasso, mas sem valor intrínseco, penso que as pessoas ainda aceitariam algo. (Estou usando a palavra escasso aqui apenas para significar oferta potencial limitada).

Mesmo se a cripto for uma moeda corrente válida, ela precisa poder competir com a moeda fiduciária e com outras moedas se ela quiser prosperar. O que faz uma moeda competitiva? Isso leva à questão mais fundamental de "O que é dinheiro?"

O Dinheiro pode criar Libertação e Civilização [...] ou Opressão

> Historicamente, o dinheiro foi uma das primeiras coisas controladas pelo governo, e a "revolução" de livre mercado dos séculos XVIII e XIX fez muito pouco efeito na esfera monetária. Portanto, é hora de voltarmos a atenção fundamental para o sangue vital de nossa economia – o dinheiro.
> – Murray Rothbard, *What Has Government Done to Our Money?*

Eu tinha sete anos de idade quando percebi que meus pais não entendiam algumas das dinâmicas mais importantes da vida. Eu estava no banco de trás do nosso carro com um saco de doces que havia sido comprado em uma loja de beira de estrada na esperança de me manter quieta. Não funcionou. Um pensamento escapou pela minha boca: "Por que pagamos por tudo? Por que as pessoas simplesmente não vão para as lojas e pegam o que precisam?"

Minha mãe respondeu: "É errado roubar."

Expliquei: "Não quero dizer roubar. Quero dizer, por que damos dinheiro às pessoas em vez de apenas compartilhar tudo?" Meus pais ficaram em silêncio.

Quando perguntei novamente, minha mãe respondeu por cima do ombro: “Não faça perguntas idiotas!”

Eles não sabiam a resposta; eu reconheci isso imediatamente. E sua incapacidade de explicar por que precisávamos de dinheiro me perturbou porque eles discutiam sobre dinheiro constantemente. Havia o suficiente para consertar o carro e para pagar a hipoteca? Eles poderiam se dar ao luxo de substituir o telhado? Qual foi o teto de gastos no Natal deste ano? O dinheiro era um tema em todos os aspectos de suas vidas e ainda assim meus pais não sabiam como responder à pergunta básica do porquê precisamos dele.

“O dinheiro é como o mundo funciona”, meu pai finalmente explicou, “porque permite que as pessoas comprem as coisas de que precisam para viver.” Esta foi uma não-resposta porque me fez não entender por que compramos coisas em vez de simplesmente compartilhá-las. Em um nível infantil, eu estava tentando entender a teoria monetária, e tenho lutado com isso desde então.

Nada foi mais benéfico nesta busca do que o pequeno livro *What Has Government Done to Our Money?* por Rothbard. Ele não usou o termo “terceira parte confiável” ou seu equivalente no livro ou em qualquer outro lugar em seus escritos, até onde eu saiba. Murray era um amigo e mentor, no entanto, o que me dá alguma confiança em prever qual teria sido sua provável reação a toda a hipótese de Satoshi. Suspeito que ele não teria visto a necessidade de confiar em um intermediário financeiro como um problema porque os bancos privados podiam oferecer garantias como reputação, resgate em ouro e auditorias. Para Murray, o dilema do dinheiro moderno parecia começar com a moeda fiduciária do governo como o problema, e terminou com o livre mercado como a solução que permitia às instituições financeiras privadas e à moeda emitida por indivíduos, caso optassem por fazê-lo. O nome de Murray para sua própria moeda hipotética era “The Rothbard”.

What Has Government Done to Our Money? Pertence aos anos pré-Bitcoin, mas oferece contribuições significativas para a cripto. Explica as origens do dinheiro em termos claros, bem como destaca o papel proeminente do dinheiro em estabelecer a libertação e a civilização. O livro providencia um contexto no qual apreciar a imensa liberação que é a cripto e a imensa opressão que é a moeda fiduciária. O livro é uma exposição enganosamente simples da maior fraude do mundo: a

inflação. O golpe só é possível quando as pessoas precisam de uma terceira parte confiável em assuntos financeiros e o governo usurpa esse papel por meio da lei e do banco central.

Compreender a inflação requer uma compreensão de bom senso do que é dinheiro e do que deveria ser. Isso não é pouca coisa. A teoria monetária moderna cria uma névoa de complexidade que garante que as pessoas comuns fiquem sem palavras quando confrontadas com questões básicas – mesmo aquelas que impactam profundamente suas vidas. Isso poderia ser evitado facilmente. As escolas poderiam ensinar economia prática; o governo e as instituições financeiras poderiam ser transparentes em vez de paredes de tijolos; a política fiscal poderia ser apresentada em inglês em vez de em burocratês com estatísticas e matemática impenetráveis.

Isso não acontecerá por si só. A falta de conscientização pública beneficia o monopólio monetário do estado e as escolas públicas financiadas por impostos não são propensas a ensinar a revolução contra a mão que as alimenta.

Um Breve Tour Pelo Básico

Toda sociedade comercializa bens e serviços porque a troca é uma necessidade humana. É o motor da vida econômica, uma fonte de prosperidade e a base da sobrevivência. O comércio não é um jogo de soma zero, como argumentam alguns economistas. Ou seja, se uma pessoa troca um peixe por um pão, o lucro de um comerciante não anula o do outro. O comércio é uma situação ganha-ganha porque a troca só ocorre quando uma pessoa valoriza mais o pão do que o peixe e vice-versa. Ou cada um ganha com a troca ou ela não ocorre. No processo, os comerciantes também estabelecem cooperação e, talvez, um nível de boa vontade que ajude o comércio no futuro. Isso torna o livre trocar um dos principais alicerces da sociedade civil.

Os seres humanos são tão magnificamente variados que existe uma gama diversificada de habilidades mesmo dentro de um pequeno grupo de indivíduos. Negociar essas habilidades aumenta as chances de sobrevivência tanto para o grupo quanto para cada membro dele, mas a troca direta ou troca é severamente falha, como explica Rothbard. “Os dois problemas básicos são ‘indivisibilidade’ e ‘falta de coincidência de quereres’.” “Indivisibilidade” significa que um bem de troca, como um arado, pode ser difícil ou impossível de dividir em muitas partes, o que

impede que seja trocado por várias coisas com várias pessoas. Então, nenhuma negociação ocorre. "Uma falta de coincidência de quereres" significa que Smith possui ovos e Jones possui sapatos, mas Smith quer manteiga. Assim, nenhuma negociação ocorre.

A troca indireta resolve o problema do escambo [...] até certo ponto. Smith troca seus ovos pelos sapatos de Jones porque o último pode ser trocado por uma terceira pessoa por algo que Smith *deseja*. Isso mitiga a falta de coincidência de quereres. Mais importante, para a teoria monetária, entretanto, negociações indiretas naturalmente encorajam um meio de troca a emergir. Por quê? Negociadores irão favorecer itens de escambo que são altamente desejáveis e serão aceitos por muitas pessoas. Bens altamente trocáveis tendem a partilhar de características, incluindo divisibilidade, durabilidade, fungibilidade e transportabilidade. Não coincidentemente, essas mesmas características frequentemente descrevem bom dinheiro, e elas se aplicam a cripto.

De acordo com o teorema de Mises, um item de escambo desejável é primeiro valorado por seu valor de uso. Rothbard lista algumas mercadorias que se tornam moedas. "[O] tabaco na Virgínia colonial, açúcar nas Índias Ocidentais, Sal na Abissínia, gado na Grécia Antiga, pregos na Escócia, cobre no antigo Egito, e grãos, contas, chá, moluscos e anzóis." A demanda por um bem gera uma "espiral de reforços: mais mercabilidade causa um uso mais amplo como um meio o qual causa mais mercabilidade etc. Eventualmente, uma ou duas mercadorias são usadas como meio geral – em quase todas as trocas – e essas são chamadas de dinheiro".

Moedas comumente aceitas eliminam a necessidade tanto por escambo quanto por troca indireta, as quais podem ser confusas, consumidoras de tempo e geograficamente limitadas. Moedas criam um livre mercado complexo que permite que bilhões de pessoas que não conhecem umas às outras consumam produtos ao redor do mundo. Em resumo, o dinheiro lança os seres humanos da sobrevivência para a prosperidade e possibilita o luxo do tempo para pensar, para criar arte, gozar de profundos relacionamentos e tomar conta de sua saúde. Um meio de troca é um dos fundamentos da civilização.

E então entra o governo. A moeda desempenhou um papel definidor em libertar e civilizar os seres humanos. Agora seria usada para escravizá-los.

Inflação, o Maior Roubo de Todos

O governo não produz bens e serviços no mercado para vender aos clientes que os desejam. Indivíduos fazem isso. O estado rouba riqueza dos chamados clientes, forçando-os a pagar por "bens" e "serviços", como os militares, quer queiram ou não. A tributação é a forma mais visível de roubo. Mas está longe de ser o único motor de roubo. Ao paralisar os concorrentes que supririam as necessidades da sociedade no livre mercado, o governo também rouba oportunidades e lucros não realizados da classe produtiva das pessoas.

A ferramenta mais poderosa de roubo público, no entanto, é o monopólio do estado na emissão de dinheiro ou fiduciário. Rothbard explica: "O surgimento do dinheiro, enquanto um benefício para a raça humana, também abriu uma rota mais sutil para a expropriação governamental de recursos […] [Se] o governo puder encontrar maneiras de se envolver em falsificação – a criação de dinheiro novo do nada – ele pode rapidamente produzir seu próprio dinheiro sem se dar ao trabalho de vender serviços ou minerar ouro. Ele pode então se apropriar de recursos astutamente e passar quase desapercebido, sem despertar a hostilidade desencadeada pela tributação."

A parte "quase desapercebida" da análise anterior é fundamental. Todo mundo entende de tributação porque vem com formulários para preencher, deduções de um salário, prisão por sonegação, agentes assustadores que auditam e um acréscimo doloroso sobre mercadorias na caixa registradora. Quase todo mundo se ressente da tributação; surtos de resistência, rebeliões e pedidos de revogação são temas comuns ao longo da história; a Revolução Americana é um exemplo. Previsivelmente, o governo quer reduzir a presença de multidões enfurecidas que protestam contra suas políticas nas ruas. No entanto, ele precisa dessa riqueza.

Em contraste, uma espiral complexa e arcana de inflação raramente enfurece a pessoa comum que não a percebe até que os efeitos sejam aparentes, ruinosos e inescapáveis. Se a tributação é o equivalente ao roubo com uma arma apontada para a cabeça das pessoas, então a inflação é um ladrão que despoja suas casas na madrugada. A inflação também é difícil de evitar porque os monopólios governamentais incorporaram o decreto e o sistema bancário central no centro do comércio moderno. Talvez o conhecido ditado deva ser "nada é inevitável, exceto a morte e a inflação".

O que é inflação? A inflação é um aumento na oferta de dinheiro e de crédito. Geralmente ela está associada ao governo, e com razão, mas também pode ocorrer com o dinheiro do livre mercado. A oferta de ouro pode aumentar por vários motivos, incluindo enormes descobertas minerais ou uma liberação maciça de reservas de um banco. Mas uma diferença crucial entre a inflação do estado e o livre mercado é que o ouro cumpre com muitos usos não monetários. Se a oferta aumentar, o consumo para esses usos também aumentará, pois o custo do ouro cairá. Isso significa que uma inflação nas unidades de ouro disponíveis seria uma coisa boa para algumas pessoas – especificamente para aqueles que usam ouro de maneira não monetária. Por sua vez, o aumento da demanda por ouro não monetário absorveria o "excesso" de oferta e elevaria o valor monetário. A inflação de livre mercado é autoajustável e é acompanhada por um benefício social, incluindo um aumento no valor de moedas privadas concorrentes, como a prata.

Por outro lado, o único uso da moeda fiduciária é como dinheiro. Isso significa que não há mecanismo de autoajuste. Os mercados mundiais podem desvalorizar uma moeda fiduciária notória se outras moedas fiduciárias não forem ainda piores. Nessa circunstância, no entanto, o governo com moeda desvalorizada pode aumentar sua impressora e criar um círculo vicioso de inflar ainda mais a oferta monetária. A inflação fiduciária não é autoajustável nem oferece benefícios a ninguém, exceto a classe de elite que recebe primeiro o dinheiro recém-impresso.

Para a pessoa média, a palavra "inflação" é sinônimo de "aumento de preços", mas o aumento é uma consequência da inflação, não um sinônimo dela. Como observado anteriormente, a inflação é simplesmente um aumento na oferta de dinheiro e de crédito. A diferença entre esses dois significados é muito mais do que semântica. Ver a inflação como um aumento de preços ignora muito do grande dano infligido pela inflação porque implica que toda a sociedade enfrenta a mesma desvantagem: preços mais altos onipresentes. O oposto é verdadeiro. A inflação é uma arma de classe que redistribui a riqueza das pessoas médias para a elite da sociedade. Isso acontece porque o novo fiat é inicialmente avaliado na mesma proporção que as unidades antigas que já estão em circulação. Dobrar a oferta de dinheiro da noite para o dia acabaria colapsando o poder de compra de cada unidade em circulação, mas o prazo operacional é "eventualmente". Os primeiros usuários aproveitam o valor da pré-inflação porque o dano escorre lentamente

por toda a economia. Esses primeiros usuários incluem o estado, a burocracia, as instituições financeiras e as empresas compadres que recebem empréstimos favoráveis. O usuário final é a pessoa comum que recebe a moeda fiduciária diluída que perdeu poder de compra à medida que se espalhava pela economia. A pessoa comum suporta o peso da inflação por ter o valor de sua riqueza e renda caindo enquanto o custo de vida dispara. Enquanto isso, a classe alta goza de maior prosperidade às custas de todos.

Com leis de curso legal e sem o padrão ouro, pouco previne o governo de expandir o dinheiro e o crédito à vontade, usando taxas de juros para afinação. Os incentivos estão todos no lado da inflação. É altamente lucrativo ao estado e na maior parte invisível para o público, especialmente nos primeiros estágios. O vilão econômico dos defensores do livre mercado, John Maynard Keynes, soube bem disso. Seu livro pivô *The Economic Consequences of Peace* declara:

> É dito que Lenin declarou que a melhor maneira de destruir o Sistema Capitalista era perverter a moeda. Através de um contínuo processo de inflação, o governo pode confiscar, secretamente e de forma não observada, uma importante parte da riqueza de seus cidadãos. A partir desse método eles não apenas confiscam, mas o fazem arbitrariamente; e enquanto o processo empobrece muitos, ela na verdade enriquece alguns. Enquanto a inflação procede e o valor real da moeda flutua selvagemente de mês para mês, todas as relações permanentes entre devedores e credores, os quais formam o fundamento último do capitalismo, tornam-se tão totalmente desordenados que são quase sem sentido; e o processo de obtenção de riqueza degenera em jogo e loteria.
>
> Lênin certamente estava certo. Não há meio mais sutil e seguro de derrubar a base existente da sociedade do que corromper a moeda. O processo envolve todas as forças ocultas da lei econômica do lado da destruição, e o faz de uma maneira que nem um homem dentre milhões de homens é capaz de diagnosticar.

Os danos da inflação continuam. Rothbard enfatiza um menos discutido:

> Isso distorce a pedra angular da nossa economia: o cálculo empresarial. Como nem todos os preços mudam uniformemente e na mesma velocidade, torna-se muito difícil para as empresas separar o duradouro do transitório e avaliar verdadeiramente as demandas dos consumidores ou o custo das suas operações. Por exemplo, a prática contábil insere o "custo" de um ativo no valor que a empresa pagou por ele. Mas se a inflação intervir, o custo de reposição do ativo quando se desgastar será muito maior do que o registrado nos livros. Como resultado, a contabilidade das empresas irá superestimar seriamente seus lucros durante a inflação – e pode até estar consumindo capital enquanto pensa estar aumentando seus investimentos.

Os bancos centrais têm grande culpa pelo roubo e distorções da inflação; o estado é, em última análise, o culpado. Um banco central é uma câmara de compensação de moeda nacional; é um intermediário para as políticas financeiras de uma nação. Ele goza de controle monopolista sobre a produção e distribuição de dinheiro e crédito de uma nação. Normalmente, também esculpe a política monetária por meio de mecanismos, como a fixação de taxas de juros, e policia os bancos membros.

O Federal Reserve System americano às vezes é chamado de "privado". Por um lado, os Bancos de Reserva regionais são corporações privadas de propriedade dos seus bancos membros. O rótulo é ilusório. O Federal Reserve foi estabelecido por um ato do Congresso em 1913 e deriva o seu poder principal de um monopólio garantido pelo governo para emitir curso legal. O sistema pode imitar uma agência privada em alguns modos, mas, como explica Rothbard, o sistema de bancos é "sempre dirigido por oficiais apontados pelo governo, e servem como braços do governo."

O Federal Reserve permite a inflação. Ele o faz de duas maneiras básicas: removendo as restrições à inflação e direcionando a própria inflação. Rothbard esboçou uma implantação inicial da primeira tática. "[O] Federal Reserve Act compele os bancos a manter a proporção mínima de reservas para depósitos e, desde 1917, essas reservas só podiam consistir em depósitos no Federal Reserve Bank. O ouro não podia mais

fazer parte das reservas legais de um banco; tudo teve que ser depositado no Federal Reserve Bank". Rothbard ilustra a segunda tática de direcionar a inflação. "Ao controlar as 'reservas' dos bancos – suas contas de depósito no Banco Central. Os bancos tendem a manter uma certa proporção de reservas para seus passivos totais de depósito, e nos Estados Unidos o controle do governo é facilitado pela imposição de uma proporção mínima legal ao banco. O Banco Central pode estimular a inflação, então, despejando reservas no sistema bancário, e reduzindo o índice de reservas, permitindo assim uma expansão do crédito bancário nacional."

Na medida em que o governo aperta as rédeas sobre o dinheiro, a liberdade e a civilização são enfraquecidas. O dinheiro privado tradicional confronta e supera a fiat do governo. Mas enquanto o estado puder dominar e manipular o dinheiro, ele pode possuir o sistema financeiro ao ponto de chegar em contas bancárias individuais, títulos e outras riquezas armazenadas de indivíduos. Ele pode possuir sua riqueza futura diluindo-a através da inflação. Até as criptos, o anarquismo tropeçou e caiu sobre o problema de terceiras partes confiáveis do estado e dos bancos. Até as criptos, o estado parecia ter um controle inabalável da moeda.

Liberdades Civis e Bancos Centrais

O sistema bancário central deve ser rejeitado não apenas por motivos econômicos, mas também por motivos de liberdade civil. (Nota: Eu não faço distinção entre direitos econômicos e civis. Ambos são expressões da propriedade de si; essa é a jurisdição moral que todo ser humano tem sobre seu próprio corpo e ações pacíficas simplesmente em virtude de ser humano. Mas fazer uma distinção entre direitos econômicos e civis é comum)

O sistema bancário central é um veículo de controle monetário e financiamento para todos no poder. De acordo com o *Financial Times* –, "Os principais bancos agora possuem um quinto da dívida total do governo". Os seis principais bancos centrais "que embarcaram na flexibilização quantitativa na última década – o Federal Reserve dos EUA, o Banco Central Europeu, o Banco do Japão e o Banco da Inglaterra, juntamente com os bancos centrais suíços e suecos – agora detêm mais de US $15 trilhões em ativos, de acordo com a análise do FT do FMI e dos números do banco central, mais de quatro vezes o nível pré-crise".

A flexibilização quantitativa ocorre quando um banco central compra títulos, geralmente do governo, para reduzir as taxas de juros e aumentar a oferta de moeda. Isso alimenta artificialmente a economia, reduzindo os custos de empréstimos para famílias e empresas. Mas isso é insustentável.

Governos e bancos centrais não são independentes. A história revela que o conluio entre eles é inerente e íntimo, não acidental. O sueco Riksbank é amplamente considerado como o primeiro banco central. Inaugurado em 1668, o Riksbank era tecnicamente um banco privado de ações conjuntas, mas funcionava sob estrita autoridade real; o rei determinou as regras de operação e nomeou a administração do banco. Todo o propósito do Riksbank era emprestar fundos ao governo e ser uma câmara de compensação para o comércio.

Em 1694, a Governança e a Companhia do Banco da Inglaterra foram criadas pelo Royal Charter. É um modelo sobre o qual a maioria dos bancos centrais se baseiam. O Banco da Inglaterra surgiu porque o crédito do rei William III estava mal. A sociedade por ações forneceu um caminho para o rei arrecadar os fundos públicos que lhe permitiram continuar travando a guerra. William III estava em desacordo militar com a Irlanda, Escócia e América do Norte, todos em vários estágios de rebelião. Mais importante ainda, no entanto, a Guerra dos Nove Anos (1688-1697) com a França devastou a marinha da Inglaterra. Nenhuma instituição financeira arriscaria as 1,2 milhões de libras necessárias para reconstruí-la.

Assim, a lei inglesa estabeleceu incentivos artificiais para encorajar empréstimos ao rei. Aqueles que auxiliam no processo foram incorporados como coproprietários do Banco da Inglaterra. Os credores davam dinheiro vivo congelado ao rei em troca do qual recebiam acesso exclusivo às finanças do governo. O banco também se tornou a única empresa de responsabilidade limitada autorizada a emitir notas, usando títulos do governo como garantia. Em outras palavras, o Banco da Inglaterra concedeu um empréstimo a um beneficiário que ninguém mais tocaria; adquiriu títulos do rei – o destinatário intocável; com base nos títulos, o banco emitiu dinheiro que foi emprestado novamente. Sem privilégio legal, o banco central não teria atraído investidores ou finanças. Com o privilégio legal, os £1,2 milhão foram arrecadados em menos de duas semanas.

Governo e bancos centrais lavam as mãos uns dos outros.

O ganho financeiro não é o único motivo para atrair pessoas para a terceira parte confiável dos bancos centrais. Há também a sede por poder. A guerra é o último desdobramento de poder através do qual os governos mantêm, asseveram e expandem a si mesmos. A guerra requer dinheiro – muito. A questão é sempre como conseguir o suficiente. Existe a opção do roubo descontrolado, é claro. A economia pode ser saqueada, mas os indivíduos saqueados podem objetar e se rebelar. Tal rebelião levou à Carta Magna em 1215; um comentador da época advertiu ao rei João, "Com as ocasiões de suas guerras, ele os pilha [o povo e os nobres] com impostos e impostos até os ossos". João foi forçado a assinar a Carta Magna, presumivelmente sob ameaça de morte. Ele prometeu parar de pilhar a economia para pagar por suas guerras. Era necessária mais sutileza na pilhagem.

Quando um governo declara guerra, ele o faz em pelo menos três frentes: o governo oponente, o povo da nação oponente e os dissidentes dentro de sua própria população. Alguns dissidentes internos agitam, a princípio, mas suas fileiras são engrossadas por aqueles que se opõem aos impostos e outras violações da liberdade civil cometidas em nome da guerra. Para o governo, a questão complicada é: como extrair o máximo de dinheiro possível sem incorrer em uma reação negativa? Como isso pode contornar a tendência das pessoas de afirmar suas liberdades civis e resistir?

Um aspecto pouco discutido dos bancos centrais e da manipulação da moeda é seu impacto nas liberdades civis. Impostos diretos, confiscos e regulações são visíveis. As pessoas entendem uma mão que vai direto para seus bolsos ou as joga na cadeia por se recusarem a pagar impostos pela guerra. Por outro lado, políticas monetárias confusas e não transparentes são invisíveis. As pessoas não entendem nem sentem imediatamente o impacto da flexibilização quantitativa, por exemplo. Elas não os levam para as ruas com placas de piquete. Em vez disso, as pessoas seguem suas vidas diárias e simplesmente assumem o ônus de um imposto indireto que não entendem muito bem.

Para reafirmar este ponto através de um paralelo: A inflação é um imposto oculto que as pessoas tendem a tolerar mesmo que se rebelem contra um imposto direto. A inflação é, no entanto, comparativamente invisível e não compreendida. As pessoas que protestariam contra um imposto pró-guerra toleram as políticas do banco central, sem as quais a guerra seria impossível. Aqueles que são antiguerra devem pedir, em primeiro lugar, a dissolução do Federal Reserve e de todos os outros

bancos centrais. Mas o papel dos bancos centrais no financiamento da guerra é invisível, o que permite ao governo evitar um confronto com ativistas antiguerra. As pessoas não reivindicam seus direitos civis por nenhuma outra razão além de não saberem que esses direitos estão sendo violados. O papel dos bancos centrais no controle social permanece em grande parte desconhecido porque é misterioso.

A Tecnologia Encontra a Anarquia, e Ambos Lucram

> "O Bitcoin é o catalisador para uma anarquia pacífica e libertadora. Foi feito como uma reação contra governos corruptos e instituições financeiras. Não foi somente criado em prol de melhorar a tecnologia financeira. Mas algumas pessoas adulteram a verdade. Em realidade, o Bitcoin era para funcionar como uma arma monetária, como uma criptomoeda posta para minar autoridades. Agora, ele está eufemizado. É visto como uma tecnologia educada e despretensiosa para apaziguar políticos, banqueiros e mães corujas. Seu propósito às vezes é ocultado para tornar a tecnologia palatável para as massas ignorantes e a elite do poder. No entanto, ninguém deve esquecer ou negar porque o protocolo foi escrito."
> – Sterlin Lujan

A cripto foi criada para fazer uma diferença política e não para obter lucro. Se os principais desenvolvedores quisessem colher uma fortuna, não teriam empregado software de código aberto e evitado as patentes que os tornariam bilionários. Lucrar com cripto e blockchain são subprodutos louváveis para alguns, e aqueles que acumularam riquezas no livre mercado devem ser aplaudidos. Isso é especialmente verdade porque a maneira como eles ganharam dinheiro não interferiu na privacidade e na liberdade financeira de ninguém. Da mesma forma, a blockchain não foi forjada para tornar o sistema bancário mais eficiente, mas para torná-lo obsoleto. Qualquer um que acredite que o Bitcoin foi designado para ganho financeiro não está prestando atenção à sua história ou ao idealismo embutido em seus algoritmos. O Bitcoin foi concebido como um veículo para criar mudanças políticas e sociais, empoderando indivíduos e empobrecendo o governo. Seus desenvolvedores eram revolucionários. O Bitcoin foi seu golpe de abertura.

E não foi sequer um momento antes da hora. A Internet deu ao governo uma arma incrível contra a privacidade dos indivíduos, que teria sido radicalmente reduzida sem a criptografia – a arte da comunicação secreta.

A História do Bitcoin

A história do Bitcoin às vezes é rastreada até o engenheiro e cientista Timothy C. May. O "Manifesto Cripto-Anarquista" (1988) de May apareceu pela primeira vez sendo distribuído por alguns tecno-anarquistas na conferência Crypto '88. O manifesto de seis parágrafos exige uma tecnologia de computador baseada em protocolos criptográficos que "alterariam completamente a natureza da regulamentação governamental, a capacidade de tributar e controlar as interações econômicas, a capacidade de manter a informação em segredo e até alterar a natureza da confiança e reputação … A tecnologia para essa revolução – e certamente será uma revolução social e econômica – existiu em teoria na última década.… Mas só recentemente as redes de computadores e os computadores pessoais atingiram velocidade suficiente para tornar as ideias praticamente realizáveis."

O manifesto conclui com um grito de guerra. "Levante-se, você não tem nada a perder a não ser suas cercas de arame farpado!"

Mesmo em 1988, May podia contar com uma rica história das criptos. Em meados da década de 1970, a criptografia deixou de ser domínio quase exclusivo das agências militares e de inteligência, que operavam em grande parte em sigilo. Em contraste, a pesquisa acadêmica que mais tarde surgiu foi abertamente compartilhada. Um evento em particular quebrou o controle do governo em campo. Em 1975, o guru da computação Whitfield Diffie e o professor de engenharia elétrica Martin Hellman inventaram a encriptação de chave pública e publicaram seus resultados no ano seguinte no ensaio "New Directions in Cryptography". (O que pode ser disputado porque a chave pública foi uma reinvenção, pois os britânicos haviam desenvolvido essa encriptação anteriormente, mas foram silenciados sobre o assunto pelo governo). Em 1977, os criptógrafos Ron Rivest, Adi Shamir e Leonard Adleman criaram o algoritmo de encriptação RSA, aquele que foi um dos primeiros sistemas práticos de chave pública.

A encriptação de chave pública atingiu a comunidade de computadores como uma explosão. Seu brilho é sua simplicidade. Cada usuário tem duas chaves – uma pública e uma privada – ambas únicas. A chave pública embaralha o texto de uma mensagem que pode ser decifrada apenas pela chave privada. A chave pública pode ser jogada ao vento, mas a chave privada deve ser bem guardada. Na época, o resultado estava próximo de uma privacidade impenetrável.

Diffie se inspirou no problema das terceiras partes confiáveis. O livro *High Noon on the Electronic Frontier*: *Conceptual Issues in Cyberspace* (1996) o cita dizendo: "Você pode ter arquivos protegidos, mas se uma intimação fosse enviada ao gerente do sistema, daí não viria nada de bom. Os administradores o dedurariam, porque não teriam interesse em ir para a cadeia." Sua solução foi eliminar a necessidade de confiança por meio de uma rede descentralizada na qual cada indivíduo possui a chave matemática de sua própria privacidade – o direito mais ameaçado pela sociedade digital. A encriptação de chave pública também removeu a tensão de enviar informações seguras por canais inseguros. Excluiu "Eve"; esse é o nome que os criptógrafos chamam de bisbilhoteiro indesejado que pode ser o estado ou um criminoso comum. É importante ressaltar que a criptografia de chave pública era gratuita para todos porque uma revolução bem-sucedida não requer nada além de participação.

O governo não achou graça. A Agência de Segurança Nacional (NSA) não podia mais espionar à vontade porque seu monopólio doméstico de criptografia foi subitamente arrancado. O jornalista Steven Levy comentou em um artigo da *Wired*: "Em 1979, Inman [então chefe da NSA] deu um discurso que veio a ser conhecido como 'the sky is falling', alertando que 'atividades criptológicas e publicações não governamentais […] representam riscos claros para a segurança nacional'."

Uma declaração posterior do criptógrafo John Gilmore capturou a resposta dos rebeldes:

> Mostre-nos. Mostre ao público como sua capacidade de violar a privacidade de qualquer cidadão evitou um grande desastre. Eles estão restringindo a liberdade e a privacidade de todos os cidadãos para nos defender contra um bicho-papão que eles não explicaram. A decisão de literalmente trocar nossa privacidade é uma decisão que deve ser tomada por toda a sociedade, não unilateralmente por uma agência de espionagem militar.

O que poderia ser chamado de "a primeira guerra cripto" estourou quando a NSA tentou restringir a circulação das ideias de Diffie e Hellman. A agência informou aos editores que os dois rebeldes e qualquer um que os publicasse poderia enfrentar pena de prisão por violar as leis

que restringem a exportação de armas militares. Um dos veículos de Hellman, o Instituto de Engenheiros Elétricos e Eletrônicos (IEEE), recebeu uma carta que dizia, em parte: “Percebi nos últimos meses que vários grupos do IEEE têm publicado e exportado artigos técnicos sobre *encriptação e criptologia* – um campo técnico que é coberto por Regulamentos Federais, a saber: ITAR (Regulamento Internacional de Tráfego de Armas, 22 CFR 121-128).” Ordens de mordaça foram emitidas. Legalização foi proposta. A NSA tentou controlar o financiamento para pesquisa de cripto e considerou exigir que as pessoas depositassem suas chaves privadas em um terceiro que seria vulnerável à ordem de um juiz ou à polícia. Isso teria retornado ao problema de terceiras partes confiáveis que a criptografia de chave pública pretendia evitar. Em reação, o cofundador da Electronic Frontier Foundation, John Perry Barlow, declarou: “Você pode ter meu algoritmo de encriptação […] quando você arrancar meus dedos frios e mortos da minha chave privada.”

A NSA falhou. A encriptação potente tornou-se um bem público que oferecia privacidade extraordinária aos indivíduos.

Levantem-se, Cypherpunks!

No final da década de 1980, os cypherpunks surgiram como algo semelhante a um movimento. O rótulo deliberadamente bem-humorado foi cunhado pela hacker Judith Milhon, que misturou “cipher” com “cyberpunk”. Os cypherpunks queriam a criptografia para se defender tanto da vigilância quanto da censura do estado. Eles também buscaram construir uma sociedade contra econômica como uma alternativa aos sistemas bancários e financeiros existentes. Conforme definido por seu exemplar e Anarcocapitalista Samuel E. Konkin III, a contra economia é o estudo e a prática de toda ação humana pacífica que é proibida pelo estado.

A visão dos cypherpunks foi facilitada pelo trabalho pioneiro do cientista da computação David Chaum, apelidado de “Houdini da cripto”. Três de seus artigos foram particularmente influentes.

- Correio Eletrônico não Rastreável, Endereços de Retorno e Pseudônimos Digitais” (1981) estabelece as bases para a pesquisa e o desenvolvimento de comunicações anônimas baseadas em criptografia de chave pública.

- "Assinaturas Cegas para Pagamentos não Rastreáveis" (1983) afirma: "A automação da forma como pagamos por bens e serviços já está em andamento. […] A estrutura final do novo sistema de pagamentos eletrônicos pode ter um impacto substancial na privacidade pessoal, bem como na natureza e extensão do uso criminoso de pagamentos. Idealmente, um novo sistema de pagamentos deve abordar esses dois conjuntos de preocupações aparentemente conflitantes." O ensaio clama por dinheiro digital.
- "Segurança sem Sistemas de Transação para tornar o Grande Irmão Obsoleto" (1985) descreve ainda mais dinheiro digital anônimo e sistemas de reputação com pseudônimos.

Um típico cypherpunk desconfiava e não gostava do governo, especialmente do tipo federal; a cruzada da NSA contra a encriptação privada só fortaleceu essa resposta. A maioria dos cypherpunks também abraçou a contracultura com sua ênfase na liberdade de expressão, liberação sexual e liberdade de usar drogas. Em suma, eles eram libertários civis. Um dos primeiros retratos dos radicais de codificação foi o artigo de Levy *Wired* mencionado anteriormente. Levy os chamou de "libertários techie-cum-civil". Eles eram idealistas que "esperam por um mundo onde as pegadas informativas de um indivíduo – desde uma opinião sobre aborto até o registro médico de um aborto real – possam ser rastreadas apenas se o indivíduo envolvido optar por revelá-las; um mundo onde mensagens coerentes são lançadas ao redor do globo por redes e micro-ondas, mas intrusos e federais que tentam arrancá-las da fumaça encontram apenas rabiscos; um mundo onde as ferramentas de espionagem são transformadas em instrumentos de privacidade." As apostas? "O resultado dessa luta pode determinar a quantidade de liberdade que nossa sociedade nos concederá no século XXI." O ideal não é que a liberdade lhes seja dada, é claro, mas que ela seja tomada como um direito natural.

Em 1991, Phil Zimmermann desenvolveu o Pretty Good Privacy (PGP), que se tornou o software mais popular do mundo de encriptação de e-mail. Ele via o PGP como uma ferramenta de direitos humanos e acreditava tanto nele que perdeu cinco pagamentos de hipoteca e quase perdeu sua casa para projetá-la. A versão original foi chamada de "uma teia de confiança". Zimmermann descreve este protocolo no manual do PGP versão 2.0.

> Com o passar do tempo, você acumulará chaves de outras pessoas que você pode querer designar como apresentadores confiáveis. Todos os outros escolherão seus próprios apresentadores confiáveis. E todos irão acumular e distribuir gradualmente com suas chaves uma coleção de assinaturas de certificação de outras pessoas, com a expectativa de que qualquer pessoa que a receba confie em pelo menos uma ou duas das assinaturas. Isso causará o surgimento de uma rede de confiança descentralizada e tolerante a falhas para todas as chaves públicas.

O PGP foi inicialmente distribuído gratuitamente por ser postado em quadros de avisos de computador. Zimmermann explicou: “[c]omo milhares de sementes de dente-de-leão soprando no vento” o PGP se espalhou pelo mundo. O governo percebeu, e Zimmermann foi alvo de uma investigação criminal de três anos com base na possível violação das restrições dos EUA de exportação de software criptográfico.

Saltando para 1992. May, Milhon, Gilmore e Eric Hughes formaram um pequeno grupo de fanáticos por programação que se reuniam todos os sábados em um pequeno escritório em São Francisco. Um artigo do *Christian Science Monitor* descreve o grupo como “todos unidos por aquela combinação única da Bay Area: apaixonados por tecnologia, mergulhados na contracultura e inabalavelmente libertários.”

O grupo cresceu rapidamente. Um fórum de postagem eletrônico chamado The List tornou-se seu aspecto mais ativo, com os “algoritmos das pessoas” atraindo forte apoio de nomes como Julian Assange e Zimmermann. O *Christian Science Monitor* comenta: “Os libertários radicais dominaram a lista, junto com ‘alguns anarcocapitalistas e até alguns socialistas’. Muitos tinham capacidade técnica de trabalhar com computadores; alguns eram cientistas políticos, estudiosos dos clássicos ou advogados”. Eric Hughes contribuiu com outro manifesto para o movimento. “A Cypherpunk’s Manifesto” começa, “A privacidade é necessária para uma sociedade aberta na era eletrônica”. Ele continua, “pois para a privacidade ser amplamente espalhada ela precisa ser parte de um contrato social. As pessoas precisam se juntar e implantar esses sistemas pelo bem comum. A privacidade só se estende até a cooperação de seus companheiros na sociedade.”

O grupo rapidamente encontrou uma objeção que viria a dominar o ataque do governo à encriptação privada; “maus agentes”, argumentou-se, usarão o anonimato para cometer crimes. Durante uma entrevista em 1992, um cético confrontou May. “Parece a coisa perfeita para notas de resgate, ameaças de extorsão, subornos, chantagem, informações privilegiadas e terrorismo”, ele desafiou e May respondeu: “Bem, e quanto à venda de informações que não são vistas como legais, digamos, sobre cultivo de maconha e aborto do tipo faça você mesmo”? E quanto ao anonimato desejado para denunciantes, confessionários e namoros?” E enquanto aos “bons agentes” que seriam penalizados pela remoção da criptografia privada?

Cypherpunks acreditavam que a criptografia de chave pública realmente tornava a sociedade *menos* perigosa e menos criminosa porque reduziu ou eliminou pelo menos duas grandes fontes de violência. A primeira foi o estado; sua intrusão criminosa na vida pessoal dos indivíduos poderia ser amplamente neutralizada pela privacidade efetiva. Se as trocas financeiras fossem invisíveis, por exemplo, o roubo de impostos ou o confisco seria impossível. A segunda fonte de violência era o risco associado a crimes sem vítimas, como o uso de drogas, que não eram vistos pelos cypherpunks como crimes. A encriptação de chave pública reduziu ou removeu esse risco. Encomendar drogas on-line, por exemplo, era mais seguro do que comprá-las em um beco de um bairro ruim à meia-noite.

Sem dúvida, a criptografia de chave pública poderia proteger atividades que *violavam* direitos, assim como pagar em dinheiro vivo poderia fazê-lo. No entanto, essa perspectiva era amplamente irrelevante, já que a encriptação era uma realidade que se espalharia apesar dos efeitos colaterais desagradáveis. Os Cypherpunks argumentaram que a tecnologia ou a comunidade poderiam desenvolver soluções para crimes online reais.

As Guerras Cripto Continuam

Um incidente capturou o núcleo das guerras cripto entre os cypherpunks e o estado. Gilmore decidiu salvar e divulgar as informações em documentos ameaçados pela censura da NSA. Ele distribuiu um artigo de um criptógrafo cujo trabalho a NSA havia sido fundamental para suprimir. Depois que Gilmore postou na Internet, o artigo se tornou viral. Em 1992, Gilmore apresentou um pedido de Freedom of

Information Act (FOIA) para adquirir as partes públicas de uma obra de quatro volumes de William Friedman, que às vezes é chamado de pai da criptografia americana. Os manuais já existiam há muitas décadas. Gilmore também solicitou que os outros livros de Friedman fossem tornados públicos.

Enquanto a NSA prolongava sua resposta à FOIA, Gilmore ouviu notícias fascinantes de um amigo cypherpunk. Os documentos pessoais de Friedman foram doados para uma biblioteca depois de sua morte, e eles incluem os manuscritos anotados de um livro sigiloso. O amigo simplesmente tirou o livro da estante da biblioteca e o xerocou para Gilmore. Outro dos livros sigilosos de Friedman foi encontrado em um microfilme na Boston University. Gilmore notificou o juiz no que se tornou um apelo à FOIA, para que os assim chamados documentos classificados estivessem publicamente disponíveis em bibliotecas. Antes de fazê-lo, porém, Gilmore fez várias cópias do material em questão e as escondeu em lugares obscuros, incluindo um prédio abandonado.

A NSA reagiu com extrema veemência. Eles invadiram bibliotecas e reclassificaram documentos que estavam disponíveis publicamente. O Departamento de Justiça chamou o advogado de Gilmore para dizer que seu cliente estava perto de violar o Ato de Espionagem, o qual poderia levar a uma prisão de até 10 anos. A violação: ele mostrou às pessoas um livro de uma biblioteca pública.

Por sua vez, Gilmore contatou repórteres de tecnologia no jornal. A NSA temia a publicidade, e os cypherpunks sabiam disso. Artigos críticos da NSA começaram a fluir, incluindo um na *San Francisco Examiner*. Dois dias depois, o New York Times afirmou: “A National Security Agency, a agência de espionagem eletrônica secreta do país, recuou abruptamente de um confronto com um pesquisador independente sobre manuais técnicos secretos que ele encontrou em uma biblioteca pública há várias semanas. […] [E]la disse que os manuais não eram mais secretos e que o pesquisador poderia guardá-los”. A *Aegean Park Press*, uma editora da Califórnia, rapidamente imprimiu os livros.

Os primeiros cypherpunks eram protótipos que definiram a atitude, a tecnologia e o contexto político em que grande parte da próxima geração de zelotes da cripto operou. Os objetivos eram a desobediência à autoridade injusta, contra economia, liberdade pessoal e a ruptura de um sistema corrupto por meio da criptografia.

Lições de Moral de Moedas Digitais Anteriores

> Existiram 3 fases da moeda: a baseada em mercadorias, a baseada em política e agora a baseada em matemática.
> – Chris Dixon

Versões de dinheiro digital e sistemas de transferência online existiam décadas antes do Bitcoin. A DigiCash e o e-gold estão entre os mais conhecidos, mas nenhum deles conseguiu abalar o obstinado problema de terceiras partes confiáveis. Ambos careciam do veículo essencial da privacidade e do self-banking criado por Satoshi: a blockchain. Os sistemas iniciais são úteis, entretanto, como lições de moral e realçam a elegância do Bitcoin.

DigiCash: Suas lições

Em 1983, o renomado criptógrafo David Chaum introduziu a ideia de dinheiro digital em um trabalho de pesquisa inovador. Em 1989, ele fundou uma corporação de dinheiro eletrônico chamada DigiCash, que, por sua vez, estabeleceu o sistema de pagamento eletrônico e-cash. (A moeda real foi apelidada de DigiCash). O e-cash foi chamado de "tecnicamente perfeito". Ele foi construído sobre um sistema anterior projetado por Chaum: Assinatura Cega. Essa é uma assinatura digital em que o conteúdo de uma mensagem de uma pessoa é disfarçado para que não seja visto por uma segunda pessoa que autentica a mensagem.

O processo é frequentemente descrito por uma analogia. Um eleitor quer que seu voto permaneça secreto. Para ser contado, no entanto, deve ser assinado por um funcionário eleitoral que verifica a elegibilidade do eleitor. A solução: o eleitor escreve suas credenciais do lado de fora de um envelope, embrulha a cédula marcada em papel carbono e a coloca dentro do envelope. O funcionário verifica as credenciais e assina o envelope, transferindo sua assinatura para a cédula interna; ele verifica a cédula sem saber seu conteúdo. O eleitor coloca a cédula agora autorizada em um novo envelope não marcado que é colocado em uma caixa de cédulas esperando para serem contadas. O tabulador verifica a assinatura de autenticação e o voto é registrado. O contator de votos não tem, entretanto, a menor ideia de quem colocou qualquer voto

particular. Nem o conteúdo do voto nem o próprio voto podem ser ligados até um eleitor individual. Essa é a essência de uma assinatura cega.

Em termos simples, o e-cash de Chaum se utiliza de assinaturas cegas como se segue: em um banco que lida com dinheiro eletrônico, você tem uma conta com $20 à qual uma senha dá acesso. Para sacar e-cash em quantias de $1 cada, você usa um software para gerar 20 números únicos e aleatórios de tamanho suficiente para que seja altamente improvável que alguém também os produza. O problema: você precisa que o banco verifique se cada número representa $1 em valor, mas você não quer que o banco saiba qual $1 é qual porque a moeda pode ser rastreada. Se não há nada mais, o banco pode combinar dados de saída e entrada, permitindo que ele saiba onde você compra, o que você compra, seu estilo de vida e outras informações que você deseja que permaneçam privadas.

Você mantém a privacidade "cegando" cada pedido com encriptação especial. O banco então recebe uma solicitação codificada na qual assina com uma chave privada de $1; isso afirma o valor e a autenticidade. O selo do banco converte o número no equivalente a uma moeda de $1 que pode ser usada apenas por você. É anônimo; o banco sabe quantas unidades de $1 ele estampou para você, mas não pode distinguir entre essas 20 unidades ou reconhecê-las de qualquer outra unidade de $1 que já autenticou.

Para gastar o dinheiro, você revela o número. Isso resulta em uma mensagem assinada válida que pode ser verificada pela chave pública do banco. As unidades de $ 1 são armazenadas em seu computador, esperando para serem enviadas para qualquer pessoa que aceite e-cash. Para fazer isso, você envia à pessoa um número decriptado e assinado, e ela o leva ao banco. A assinatura é verificada; o número de série é registrado; o valor é resgatado. Gravar o número permite que o banco rejeite qualquer tentativa de gasto duplo. Mas o banco não pode conectar a transação à sua conta, e o destinatário de $1 não tem ideia de quem você é, a menos que você decida revelar sua identidade.

O processo é tão anônimo quanto o dinheiro. Isso contrasta fortemente com o uso de cartão de crédito online, que envolve dizer a uma empresa e a um destinatário quem você é, onde está e o que está comprando. O DigiCash também está protegido contra pessoas maliciosas que estão tentando roubar identidades. Ele tem uma vantagem extra. Porque ele é altamente divisível, ele acomoda micro pagamentos – pagamentos menores de $10, para a qual os custos de transação fazem dos

cartões de crédito virtualmente impraticáveis. O e-cash era perfeito para transferir e-nickels e e-quarters pela Internet.

A DigiCash Inc. causou um grande impacto na comunidade financeira. O primeiro banco a adotá-lo foi o Mark Twain Bank em St. Louis, Missouri, mas outros logo se seguiram. Em 1998, o e-cash estava disponível através do Deutsche Bank na Alemanha, Credit Suisse na Suíça e vários outros pontos de venda poderosos. Mas, em 1998, a DigiCash Inc. entrou com pedido de falência do Capítulo 11 e posteriormente vendeu seus ativos, incluindo as patentes.

O que aconteceu? As explicações variam e todas podem conter alguma verdade.

Em uma entrevista de 1999, Chaum afirmou que o DigiCash foi uma ideia antes de seu tempo porque o comércio eletrônico não estava firmemente estabelecido. A *Forbes* teve outra explicação: “Uma admirável moeda nova para um admirável mundo novo, com apenas um problema: Ninguém queria isso – nem bancos, nem comerciantes e, mais importante, nem consumidores. O comércio eletrônico está florescendo, mas acontece que Visa e MasterCard – não dinheiro digital – são a moeda de escolha.” A maioria dos governos estavam entre aqueles que não gostaram da moeda irrastreável porque ela poderia ser usada para sonegar impostos e cometer outros “crimes” geralmente contra o estado.

Em uma fascinante peça anônima na *Next Magazine*! foi apresentada uma teoria totalmente diferente. Os criptógrafos, explica, são geralmente paranoicos. E Chaum é um GRANDE criptógrafo. O funcionamento interno do DigiCash descrito no artigo parece uma ala psiquiátrica, não uma empresa de tecnologia. Chaum é também comparado como um homem de negócios abismal. Um exemplo:

> ING Investment Management estava interessado. Este acordo foi de cerca de vinte milhões de guilders [US $ 10 milhões de dólares na época]. Os planos estavam todos traçados. O ING Barings, juntamente com o Goldman Sachs, também levaria o DigiCash ao mercado de ações dentro de dois anos. “No dia em que estávamos prontos para assinar, David não queria”, conta Stofberg [o homem responsável pelos assuntos financeiros da DigiCash].
> “Ele era tão paranoico, que sempre achava que algo estava errado. Havia 8 pessoas do ING, incluindo o CEO, e David simplesmente se recusou a assinar”!

Uma abordagem mais interessante do que psicologizar é observar algumas das fraquezas dos sistemas de e-cash e DigiCash, que contribuíram para seu fracasso e compará-los com o sucesso do Bitcoin e da blockchain.

- Chaum acreditava em patentes e direitos autorais, ambos aplicados em seus projetos. Isso restringiu severamente o acesso e o desenvolvimento cooperativo por uma comunidade global de mentes brilhantes. Colocar uma etiqueta de preço no produto dificultou a ampla aceitação do público. Por outro lado, o Bitcoin é livre de patentes e é opensource, o que dá acesso irrestrito e permite que o desenvolvimento avance.
- O e-cash não evitou o problema de terceiras partes confiáveis porque precisava de uma assinatura cega de autorização de uma instituição financeira. Além do mais, sua crescente aliança com bancos centrais proeminentes indicava uma presença crescente de terceiras partes confiáveis. O Bitcoin peer-to-peer elimina completamente terceiras partes confiáveis devido ao fato que a aceitação pela blockchain *é* a autorização, e cada participante é um self-banker.
- O e-cash exigia um emissor centralizado, como um banco. O Bitcoin é descentralizado até o nível individual.
- O e-cash preservou o sistema bancário existente. Bitcoin torna o sistema atual irrelevante.
- E-cash era vulnerável às falhas de personalidade de um homem. A comunidade Bitcoin é assombrada por conflitos internos, mas nenhuma personalidade pode destrui-la porque ninguém é dono do sistema. Além disso, sempre é possível criar uma criptomoeda alternativa para competir com uma que seja inferior de alguma forma.
- O e-cash não foi projetado para libertação financeira. O ensaio “Untraceable Electronic Cash”, de coautoria de Chaum, afirmou: “Gerar um dinheiro eletrônico deve ser difícil para qualquer pessoa, a menos que seja feito em cooperação com o banco”. Os anarquistas e idealistas que esculpiram o Bitcoin queriam empoderar o indivíduo contra os bancos e o estado e não precisavam da permissão de ninguém para fazê-lo.

Sem dúvida que as corporações mostraram interesse imediato em e-cash. Eles só recentemente mostraram interesse no Bitcoin, que agora esperam patentear, dominar e domar para seus próprios propósitos.

E-gold: Suas lições

E-gold era um sistema de moeda de ouro digital que foi operado entre 1996 e 2009 pela Gold & Silver Reserve, Inc. Em 2000, a G&SR se reestruturou e uma nova empresa, e-gold Ltd., assumiu a administração da emissão e de transferências de e-metal. A moeda digital estava ligada ao ouro, com a unidade de conta típica sendo gramas ou onças troy. Como os primeiros certificados de ouro dos EUA, o e-gold representava unidades de ouro para as quais poderia ser resgatado sob demanda do metal armazenado.

Clientes com contas no site do e-gold também podiam fazer transferências instantâneas de metais preciosos para outras contas.
Foi um dos primeiros sistemas de pagamento a permitir trocas globais complexas fora do sistema bancário tradicional. Um crítico da moeda fiduciária e dos bancos convencionais, o cofundador e libertário Douglas Jackson tinha uma missão; ele queria forjar uma alternativa privada ao lamaçal financeiro causado pelos governos. No livro *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (2016), o editor da revista *Digital Gold*, P. Carl Mullan, citou Jackson como dizendo que tal "tarefa exigia capacidade computacional em larga escala, armazenamento de dados e meios de comunicação globais seguros". Os custos eram proibitivos, exceto para os governos nacionais. Isto é, até a Internet.

Com a Internet, o e-gold foi pioneiro em vários avanços. Em 1999, por exemplo, a empresa introduziu pagamentos móveis sem fio usando um celular habilitado para web. Isso foi sete anos antes do PayPal oferecer um serviço semelhante. Uma inovação menos louvável veio em 2000, quando a empresa exigiu que os clientes que desejassem agregar valor às suas contas tivessem uma terceira parte confiável e independente que pudesse trocar e-gold por moeda e vice-versa. Em um ano, várias dezenas de empresas e indivíduos preencheram esse nicho; uma nova indústria nasceu.

De acordo com a e-gold Ltd., o número de contas cresceu de 1 milhão em 2003 para 5 milhões em 2008. Usuários de e-gold tinham

uma variedade de motivos. Alguns eram fanáticos por ouro que acreditavam devotamente que o e-gold era superior a moeda fiduciária. Outros eram anarquistas econômicos que pensavam que o governo não tinha papel adequado para desempenhar no dinheiro. Outros ainda queriam sonegar impostos ou minimizar os riscos de crimes sem vítimas.

Muitos mais inundaram os emergentes Programas de Investimento de Alto Rendimento, alguns dos quais usavam e-gold como uma plataforma de pagamento. Esses programas ofereciam altos retornos irrealistas que só poderiam ser mantidos redirecionando a riqueza de novos investidores; os esquemas Ponzi levaram a uma corrida do ouro eletrônico a um nível internacional. Os fraudadores aproveitaram os recursos do e-gold, como o fato de que todas as transações eram finais e nunca eram estornadas. Os golpistas abriram contas de e-gold e pediram aos potenciais investidores que fizessem o mesmo. Em seguida, eles extraíram dos investidores e compradores tudo o que podiam.

A essa altura, o e-gold oferecia uma ampla gama de serviços, desde cassinos e leilões online até comércio de metais e doações para organizações sem fins lucrativos. A empresa estava repleta de possibilidades para golpistas. Infelizmente, os clientes fraudados muitas vezes não faziam distinção entre o próprio e-gold ético e os vigaristas que os roubavam com investimentos falsos ou com bens inexistentes. Alguns usuários desiludidos reclamaram com as autoridades governamentais.

Em 2007, o governo federal dos EUA acusou o e-gold de lavagem de dinheiro e violação de 18 leis dos EUA. Código §1960, o qual proíbe as empresas de transmitirem moeda sem uma licença. Muitas corretoras atreladas ao e-gold foram fechadas. A publicidade e as corretoras perturbadas causaram uma queda íngreme no número de clientes e-gold; a dificuldade de trocar e-gold por moeda fiduciária fez com que potenciais recebedores de e-gold fugissem. Muitos clientes ficaram presos com contas que não podiam liquidar.

O e-gold lutou vigorosamente contra as acusações, sem sucesso. Em Abril de 2008, o juiz em *United States of America v. E-gold, Ltd*, decidiu contra a companhia e, ao fazer isso, dramaticamente aumentou o alcance de autoridade do Departamento do Tesouro. A lei agora definia um “transmissor de dinheiro” como um negócio que transferia qualquer valor armazenado de uma pessoa para outra, mesmo que a transferência envolvesse dinheiro. Este foi um cheque em branco para processos futuros.

Os três diretores da empresa se declararam culpados e firmaram um acordo pelo qual o e-gold cumpriria os requisitos legais para um negócio de transmissão de dinheiro, incluindo ser licenciado. Jackson recebeu 300 horas de serviço comunitário, 3 anos de supervisão e uma multa de US $200. Ele poderia ter recebido 20 anos e uma multa de US $500.000. Os outros dois diretores receberam a mesma sentença, com multas mais pesadas.

Então veio uma amarga ironia. As confissões de culpa impediram os diretores de adquirir uma licença em qualquer lugar nos EUA. Isso colocou todo o e-gold em bloqueio porque devolver dinheiro aos clientes envolveria a transmissão de dinheiro sem licença, o que violava o acordo judicial. Em 2010, o governo finalmente permitiu que o e-gold devolvesse o valor monetizado de suas contas aos clientes.

A definição expandida e vaga do Tesouro de "transmissor de dinheiro" tem implicações claras para o bitcoin. O sucesso do e-gold e o processo judicial contra ele mudaram a forma como o governo lidava com os sistemas de pagamento online. Agora tinha o precedente legal para agir contra a cripto.

Os paralelos entre Bitcoin e e-gold são claros. O ouro eletrônico era altamente divisível em micro pagamentos tão pequenos quanto um décimo de milésimo de grama. Mantinha um registro aberto no qual as transações diárias eram publicadas ao vivo e de forma transparente. Assim como o bitcoin, o e-gold não era uma moeda complementar. Uma moeda complementar é aquela que não compete com uma moeda nacional; um exemplo seria dinheiro privado emitido como promoção por uma empresa para clientes, que poderia ser usado para comprar mercadorias na loja. O e-gold era intencionado como um substituto para a moeda fiduciária e para o sistema bancário, com a vantagem adicional de ser um escape contra a inflação.

As diferenças entre Bitcoin e e-gold são tão importantes quanto os paralelos.

- O e-gold incorporou o problema de terceiras partes confiáveis, como descobriram os clientes encurralados por processos judiciais. É difícil culpar o e-gold pelas circunstâncias, é claro, mas a desonestidade ou a ineficiência não são os únicos riscos de confiar aos outros o seu dinheiro. O Bitcoin elimina esse problema.

- Indiscutivelmente, o e-gold introduziu um "problema do quarto confiável" quando insistiu que os clientes usassem corretoras para converter e-gold na, e para fora da, moeda fiduciária.
- O e-gold e as casas de câmbio eram pontos de centralização e alvos fáceis para regulação ou proibição. Eles também eram pontos de estrangulamento para coletar informações do cliente. Quando o e-gold foi reestruturado em 2000, o OmniPay se formou como o sistema de câmbio da empresa. O OmniPay utilizou três métodos para verificar a identidade dos clientes: verificação postal universal; pagamento apenas por transferência bancária; e, salvaguardas para detectar pagamentos recebidos de terceiros. No acordo de apelo do e-gold anos depois, o governo quase certamente obteve acesso a essas informações. O Bitcoin peer-to-peer é pseudonímico.
- A insistência do e-gold na “associação para usar” restringiu a disseminação de seus serviços. O Bitcoin está aberto a todos.

O risco de uma corretora que necessita de confiança como a OmniPay é um aviso para os usuários de cripto. Uma corretora centralizada geralmente é o primeiro alvo da regulamentação do governo porque é visível, vulnerável e constitui um cachê de dados valiosos sobre usuários de outro modo ocultos. Os proprietários de corretoras provavelmente cumprirão as exigências do governo porque a não conformidade significa ser fechado, preso ou ambos. Em suma, a centralização incentiva até mesmo terceiros honestos a obedecerem a leis e regulamentos que prejudicam os clientes.

> Empresas como Visa, Dun and Bradstreet, Underwriter's Laboratories e assim por diante conectam estranhos desconfiados em uma rede de confiança comum. Nossa economia depende deles. Muitos países em desenvolvimento carecem desses centros de confiança e se beneficiariam muito com a integração com centros mundiais desenvolvidos como esses. Embora essas organizações geralmente tenham muitas falhas e fraquezas – as empresas de cartão de crédito, por exemplo, têm problemas crescentes com fraude, roubo de identidade e relatórios imprecisos, e a Barings recentemente faliu porque seus sistemas de controle não se adaptaram adequadamente à negociação de títulos digitais e muitas dessas instituições estarão conosco por muito tempo.
> – Nick Szabo.

A maior ameaça financeira à riqueza e à liberdade das pessoas é o sistema confiável de terceiros que não atende aos clientes, mas corre, em vez disso, para cumprir as regulamentações governamentais, como os requisitos de relatórios.

O anonimato é uma ferramenta poderosa para a privacidade, mas os indivíduos também precisam evitar os canais estatais que contrariam a confidencialidade. A coleta de dados moderna é voraz, e a fiscalização está acelerando. Se você jogar o jogo do estado ao seguir os caminhos financeiros, ele vai te dirigir para baixo porque o estado escreveu o livro de regras, e ele tem a vantagem da casa. Ele não irá jogar justo. Então não jogue. Para repetir Buckminister Fuller: “Você nunca muda as coisas ao lutar contra a realidade existente. Para mudar algo, construa um novo modelo que faça do modelo existente obsoleto”. Afastar-se do estado e simplesmente viver dá à liberdade a vantagem da casa. Até recentemente, no entanto, afastar-se significava um enorme sacrifício de oportunidades econômicas e de qualidade de vida porque o estado tinha uma trava no que Nick Szabo chama de “centros de confiança”.

Satoshi e Buckminister Fuller

O brilhantismo do Bitcoin: ser um novo modelo do que Fuller falou. Usuários da blockchain podem se afastar de terceiras partes confiáveis sem profundo sacrifício. A blockchain ou performa os serviços válidos de uma terceira parte confiável ou torna mais óbvia a necessidade por eles. Corretoras descentralizadas – corretoras peer-to-peer – cada vez mais providenciam serviços sofisticados tais como comprar e vender cripto como especulação.

O “White Paper” de Satoshi e o passo-a-passo do “Bitcoin Whitepaper: A Beginner's Guide” mostram como a blockchain substitui as terceiras partes confiáveis. O documento define “uma moeda eletrônica como uma cadeia de assinaturas digitais”. As moedas viajam por um registro digital distribuído, chamado blockchain, pelo qual são registradas de forma transparente, cronológica e imutável. Esses são os passos básicos na jornada de uma moeda:

1. Um indivíduo transmite uma nova transação para todos os nodes ou computadores na rede.
2. Os nodes coletam a nova transação para um bloco. Um bloco é como uma página única no registro da blockchain, ele contém informação sobre uma transferência específica, bem como está processando dados.
3. O controlador de cada node – chamado de “minerador” – performa uma proof of work para o bloco. A prova de trabalho é um cálculo de computador que é difícil de produzir em termos de poder de processamento e tempo, mas é fácil para outros verificarem.
4. Quando um node tem uma proof of work, ele transmite o bloco concluído para todos os outros nodes.
5. Os nodes aceitam o bloco somente se a transação for válida e a moeda ainda não tiver sido gasta. Timestamps exclusivos, incluídos em cada bloco, evitam gastos duplos.
6. Os nodes expressam a aceitação do bloco procedendo ao trabalho no próximo na cadeia, usando o hash do bloco previamente aceito para construir uma continuidade ininterrupta de informações. Um hash é uma função que converte uma entrada em uma string alfanumérica de tamanho fixo. Cada bloco possui um valor de hash único.

Terceiros confiáveis originalmente surgiram porque eles providenciaram funções válidas para consumidores. A função incluía verificação de uma transação, facilidade e segurança de uma transferência,

preservação da privacidade, prevenção de gastos duplos, mediação de disputas e provisão de um registro. Hoje, as terceiras partes confiáveis perverteram esses valiosos serviços aos consumidores com assaltos a eles. O Bitcoin retorna esses serviços aos indivíduos sem ataques de atendentes.

Verificação de uma transação. Uma terceira parte confiável válida autentica uma transação. Um banco pode comparar a assinatura num cheque com a que está no arquivo, ou ele pode verificar que o dinheiro não é falsificado. Esses serviços têm valor, Mas uma quantia estonteante da autenticação feita pelos bancos hoje são *des*valor para os consumidores. A exaustiva verificação da identidade de um consumidor, por exemplo, viola sua privacidade para saciar o apetite do governo por dados, o que é frequentemente usado para danificar o consumidor

A blockchain verifica transações sem se intrometer nos usuários. A transferência é autenticada, não os participantes. A transação é verificada por mineradores através de uma proof of work conduzida num bloco. Uma moeda é autenticada quando a proof of work está completa e o bloco é aceito pela blockchain. Visto que a blockchain é um registro aberto público, todos podem traçar a história de uma moeda e terem a certeza da precisão de uma transação sem saberem a identidade daqueles envolvidos. O governo pode pesquisar na blockchain, mas o registro é muito mais uma barreira do que um acréscimo na fiscalização.

Facilidade de transferência. Enquanto o comércio global galopa para frente e a internet encoraja a gratificação instantânea, a velocidade e facilidade de transferências se tornou cada vez mais importante – isto é, para o consumidor. Com um monopólio virtual sobre transferências internacionais, entretanto, os bancos definem termos que os beneficia e que prejudicam o consumidor. Bancos impõe custos diretos e indiretos. Um custo direto é a taxa associada a cada transferência, que pode ser substancial. Três custos indiretos: a conversão de moeda, se necessário; as informações pessoais necessárias; e o tempo considerável que uma transferência pode levar para ser compensada. O período de compensação é chamado de “float”. Float é o dinheiro no sistema bancário que é contado duas vezes no processo de transferir o pagamento – uma vez quando ele é depositado no banco do pagador, e uma vez quando é recebido pelo banco do pagador. Visto que o banco do pagador recebe juros sobre o dinheiro flutuando, tem havido incentivo para fazer o processo mais longo do que o necessário.

Em contraste, a blockchain não reconhece distância na transferência de riqueza ou de informações. Dois computadores na mesma casa podem estar tão próximos ou distantes um do outro (em termos de tempo de transmissão) quanto dois computadores em continentes diferentes. Os mineradores cobram uma tarifa por seu serviço, mas as tarifas são conhecidas e não têm pegadinhas ocultas. Se a tarifa de transferência de uma cripto é insatisfatória, então há muitas outras criptos para se escolher. Em contraste, tarifas bancárias tendem a ser padronizadas. A maioria das transferências ocorrem rapidamente – ao menos comparando aos bancos – e não há float aí. A blockchain não tem auto interesse ou agenda escondida.

Segurança ou transferência. Até mesmo bancos honráveis podem ser hackeados, roubados e comprometidos em suas transmissões. Embora existam muitas corretoras de cripto perdendo ou roubando a riqueza de suas contas – e esse é um problema inegável – bancos são tão vulneráveis quanto. Não há uma diferença grande entre os dois, entretanto, no que tange a segurança. Toda instituição financeira over-the-table entrega informações de clientes ao governo, que utiliza os dados para tributar, confiscar, multar e prender clientes.

A blockchain é descentralizado e resiste a ataques de hackers; não pode ser corrompida por más intenções porque é inanimada. A amplamente divulgada perda de moedas por roubo ocorre quando uma pessoa passa das transferências peer-to-peer que controla para depositar suas moedas em uma corretora, especialmente uma centralizada. A comunidade cripto precisa reduzir os riscos nessa categoria de uso das criptos. O trabalho está em andamento.

Enquanto isso, nenhuma informação pessoal é entregue ao governo. O registro é transparente para todos, incluindo ao estado, mas é relativamente fácil mascarar uma identidade e embaralhar as transferências por meio de serviços como mixers ou tumblers. A blockchain é atualmente o método mais seguro pelo qual podemos transferir fundos online. A principal ameaça à segurança é se o governo tentar controlar toda a internet. Se isso for possível e se as alternativas não surgirem rapidamente, todos os métodos de transmissão online estarão ameaçados, não apenas a criptografia.

Preservação da privacidade. O tipo de privacidade outrora notoriamente oferecido pelos bancos suíços já se foi, mesmo na Suíça. As instituições financeiras são pontos de trava nos quais os dados pessoais de um cliente são coletados e compartilhados com as autoridades. A

única privacidade verdadeira é o sigilo real com que bancos informam sobre um cliente, sem o conhecimento ou consentimento do cliente.

Manter a privacidade em uma blockchain transparente parece ser uma contradição em termos. O "Bitcoin Whitepaper A Beginner's Guide" explica o porquê não é "Com a rede peer-to-peer, a privacidade ainda pode ser alcançada mesmo que as transações sejam anunciadas. Isso é feito mantendo as chaves públicas anônimas. A rede pode ver os valores dos pagamentos sendo enviados e recebidos, mas as transações não estão vinculadas a suas identidades."

Se um usuário decidir revelar as chaves públicas, uma estratégia de privacidade comum é o pseudônimo. Uma transferência peer-to-peer não requer informações para além dos cripto endereços do remetente e do destinatário, que são gerados de forma privada pela carteira de cada participante. No entanto, quando uma pessoa se junta à blockchain, ela se torna vulnerável à análise de rede que procura padrões de transferências para montar o perfil de um usuário. É por isso que alguns usuários geram um endereço diferente para cada transação, o que cria vários pseudônimos. Satoshi explica: "Quando você gera um novo endereço bitcoin, só ocupa espaço em disco em seu próprio computador (como 500 bytes). É como gerar uma nova chave privada PGP, mas com menos uso de CPU porque é ECC. O espaço de endereçamento é efetivamente ilimitado. Não faz mal a ninguém, então gere tudo o que você quiser."

Outras práticas padrões de privacidade: crie várias carteiras para isolar uma transação ou um tipo de transação de ser associado a um padrão; encobrir um endereço IP usando uma ferramenta de anonimização como o Tor; e passe por um serviço de mixagem.

Prevenção de gastos duplos. O gasto duplo ocorre quando a mesma unidade de dinheiro é gasta em mais de uma transação, embora possa ser gasta legitimamente apenas uma vez. Satoshi descreve como os sistemas de pagamento tradicionais evitam gastos duplos: "Uma solução comum é introduzir uma autoridade central confiável, ou cunhagem, que verifica todas as transações em busca de gastos duplos. Após cada transação, a moeda deve ser devolvida à casa da moeda para emitir uma nova moeda, e apenas moedas emitidas diretamente da casa da moeda são confiáveis para não serem gastas duas vezes. O problema com esta solução é que o destino de todo o sistema monetário depende da empresa que administra a casa da moeda, com todas as transações tendo que passar por eles, assim como um banco". A solução coloca a oferta

monetária nas mãos de uma terceira parte confiável, ou mesmo de uma “quarta parte confiável”, o que o torna isso uma *não*-solução.

Em teoria, a cripto é suscetível a gastos duplos. Duas transações com a mesma moeda podem ser transmitidas em rápida sucessão para que a primeira não seja registrada publicamente antes que a segunda seja enviada. A solução de Satoshi é elegantemente simples. Toda transação não é somente pública, mas também adotada por todos os participantes da rede em uma linha do tempo para que possamos assumir que o pedido da cadeia é o mesmo para todos. Cada transação é marcada temporalmente. Se uma segunda transação com a mesma moeda ocorre, então a marca temporal inicial é contada, e a última descartada.

Mediação de Disputas. O dinheiro físico tinha uma vantagem sobre outras formas de pagamento; a troca é irreversível com exceção do consenso ou através de um processo judicial. A maioria dos sistemas de pagamento online possuem processos embutidos para reverter ou contestar uma transação. O serviço aumenta as tarifas gerais do sistema de pagamento, bem como colocam um limite prático sobre o tamanho mínimo de uma transação. Também aumenta o envolvimento prático do sistema de pagamento nas transações.

As transferências de blockchain são irreversíveis. Os fundos só podem ser devolvidos em uma base ponto a ponto se o destinatário concordar em fazê-lo. Isso inutiliza a necessidade de uma tarifa e permite micro pagamentos. Se a garantia tradicional do “dinheiro de volta” é desejada, então alguns serviços providenciam garantia por uma tarifa extra.

A provisão de um registro. Instituições financeiras mantém registros, mas seus conteúdos podem ou podem não ser providenciadas ao consumidor. A interação de um banco com uma agência fiscal, por exemplo, quase certamente será escondida de um titular da conta. Isso significa que muitos registros são mantidos apenas para benefício do banco e do governo, não para o cliente.

A própria blockchain é o registro. É um registro imutável e transparente de todas as transferências ocorridas desde o bloco original Genesis. Nenhuma interação oculta pode prejudicar um usuário.

Em resumo, a cripto fornece os serviços de um terceiro honesto com vantagens adicionais.

Satoshi é um Libertário e Anarquista?

Parte de explorar a dinâmica de terceiras partes confiáveis e a importância de contorná-los é perguntar: "Por que essa tarefa foi tão importante para Satoshi?" Ele era um libertário e anarquista ou ele era politicamente neutro e simplesmente farto de bancos? Uma declaração explícita de Satoshi sobre o assunto teria sido muito útil para responder a essa pergunta. Do jeito que a situação está, no entanto, o melhor que alguém pode fazer é examinar as evidências circundantes, como suas breves declarações on-line e o Whitepaper, e especular a partir da estrutura do próprio Bitcoin.

Em 31 de outubro de 2008, Satoshi publicou" Bitcoin: A Peer-to-Peer Electronic Cash System" (o "White Paper") na Lista de Discussão sobre Criptografia em metzdowd.com. Apresentou a tecnologia por trás do Bitcoin e o design de seu instrumento de implementação – a blockchain. A breve explicação de Satoshi é um documento tecnológico definidor do nosso século.

É ainda mais notável, portanto, que ninguém parece saber a identidade de Satoshi, se "ele" é realmente uma equipe, ou muito mais sobre ele. Claramente, ele codificou por amor à tecnologia e não por desejo de fama porque evitou os holofotes; ele também não perseguiu o status acadêmico. Como o código é de código aberto e não patenteado, a aquisição de riqueza também não era uma força motriz, embora os um milhão de bitcoins em sua conta agora constituam uma fortuna incrível. Ao contrário de May e outros antecessores, Satoshi não exibiu arrogância ou desejo de chocar; em um post, ele se desculpa e modestamente diz: "Desculpe lhes dar um balde de água fria. Escrever uma descrição dessa coisa [Bitcoin] para o público em geral é muito difícil." Em suma, ninguém pode afirmar definitivamente os motivos de Satoshi ou seu propósito final. Pelo processo de eliminação, a motivação política torna-se mais provável. Seus atos e palavras fornecem outras razões para chegarmos a essa conclusão.

Satoshi começou a escrever o código Bitcoin em 2007. Quando o "White Paper" apareceu na lista de discussão da Cryptography em 2008, também foi disponibilizado em um site criado por Satoshi – bitcoin.org. A lista de discussão consistia em especialistas em matemática, estatística e criptografia, que imediatamente argumentaram contra a viabilidade do Bitcoin. Não será escalável, alegaram; requer muitos recursos para ser prático, argumentaram. Além disso, "maus" nodes podem controlar o poder da CPU da rede e gerar uma cadeia mais longa

do que os nodes “honestos”; maus agentes poderiam controlar a blockchain.

As pacientes respostas de Satoshi gradualmente convenceram a maior parte da lista de que o Bitcoin poderia funcionar. Enquanto isso, os desenvolvimentos no lançamento aconteceram rapidamente. Os destaques incluem:

- 3 de janeiro de 2009, o bloco Genesis é extraído.
- 9 de janeiro de 2009, a versão 0.1 do software Bitcoin é lançada no Sourceforge.
- 12 de janeiro de 2009, ocorre a primeira transação de bitcoin.
- 5 de outubro de 2009, uma taxa de câmbio de US $1 = 1.309,03 BTC é estabelecida.
- 12 de outubro de 2009, o canal #bitcoin-dev é registrado para comunidades de desenvolvimento de código aberto.
- 16 de dezembro de 2009, a versão 0.2 é lançada.
- 6 de março de 2010, dwdollar estabelece uma corretora de Bitcoin.
- 22 de maio de 2010, a primeira transação no mundo real ocorre quando uma pizza é comprada por 10.000 bitcoins.
- 7 de julho de 2010, a versão 0.3 é lançada.
- 16 de outubro de 2010, ocorre a primeira transação com bitcoin como garantia.

Em meados de 2010, Satoshi transferiu a bitcoin.org para Gavin Andresen. Andresen explica:

> Comecei a enviar código para Satoshi para melhorar o sistema principal. Com o tempo, ele confiou no meu juízo sobre o código que escrevi. E, eventualmente, ele me perguntou de forma repentina se estaria tudo bem se ele colocasse meu endereço de e-mail na página inicial do bitcoin, e eu disse que sim, sem perceber que quando ele colocou meu endereço de e-mail lá, ele tirou o dele. Eu era a pessoa que todos enviavam e-mails quando queriam saber sobre bitcoin. Satoshi começou a recuar como líder do projeto e a me empurrar para frente.

Em 2010, Satoshi ficou em silêncio. Mais uma vez, fica claro que ele não escreveu pela fama.

O lançamento sistemático e meticuloso do bitcoin, bem como a estrutura elegante da blockchain, reflete um homem que pensa as situações em detalhes e entende suas implicações. Satoshi compreendeu o impacto político de seu sistema revolucionário, mas fez poucos comentários sobre o assunto.

Evidência das motivações políticas de Satoshi

Grande debate gira em torno da política de Satoshi com muitas pessoas projetando suas próprias atitudes em relação ao Bitcoin para ele. Mas todas as indicações do mundo real apontam para Satoshi ser um libertário, um anarquista ou ambos. As evidências das crenças políticas de Satoshi remontam ao bloco Genesis – o primeiro elo na blockchain. Ele contém a seguinte mensagem: "A Times de 03/Jan/2009: Chancellor à beira do segundo resgate aos bancos". A mensagem é uma manchete da primeira página do jornal britânico *The Times* de Londres. 3 de janeiro de 2009 é o aniversário do blockchain – a revelação do presente de Satoshi para o mundo. Por que ele escolheu anunciá-lo com essas palavras específicas?

Algumas pessoas pensam que o texto foi uma escolha aleatória da edição de 3 de janeiro do *Times*, e foi inserido com o único propósito de comprovar a data. Eles afirmam que a mensagem poderia facilmente ter sido "Dez profissionais do sexo presos em Sting". Esta afirmação desafia sua credibilidade. Satoshi era um programador metódico que ia diretamente ao cerne dos assuntos sem frivolidade, capricho ou apartes. Ele lançou o que ele deve ter sabido ser uma obra-prima de codificação, e não é plausível que ele tenha colocado uma mensagem aleatória no bloco Gênesis. O próprio fato de que o primeiro bloco é chamado de "Gênesis" – provavelmente uma referência ao primeiro livro da Bíblia em que Deus cria o mundo – mostra o significado que Satoshi deu ao evento.

Um cenário muito diferente é altamente provável. Satoshi está sentado em seu computador, preparando-se para lançar o primeiro bloco para o mundo como uma semente ao vento. Ele conhece seu poder e quer que as pessoas conheçam seu propósito sem ter que abrir sua concha de anonimato. Ele acabou de ler o jornal da manhã com seus rela-

tórios contínuos de torpeza financeira em que as elites políticas e financeiras agiram apenas em benefício próprio às custas dos pagadores de impostos. Uma manchete fornece o trecho perfeito sobre as duas agências mais responsáveis pelo estupro econômico dos pagamentos de impostos – o governo e o sistema bancário. As oito palavras também capturam o conluio entre eles. Satoshi digita cuidadosamente: “Chancellor à beira do segundo resgate aos bancos”, e incorpora essa mensagem no Genesis de uma dinâmica que ele acredita que pode mudar o mundo. A intenção é anti-chancellor, anti-banco e anti-resgate. Desde o primeiro piscar do blockchain, ele declara que o poder do dinheiro está sendo devolvido às pessoas.

Evidências a partir do “White Paper”

Outro ponto de debate sobre as intenções políticas de Satoshi gira em torno do tom neutro do “Whitepaper”. O documento ainda afirma que um sistema de instituições financeiras terceirizadas confiáveis “funciona bem o suficiente para a maioria das transações”. Apenas objeções práticas ao sistema existente são delineadas nele. Em suma, o “Whitepaper” não parece um manifesto político.

Nem deveria. Um whitepaper é técnico. É uma explicação oficial de uma ideia ou experimento e de seus resultados ou conclusões, que é apresentada para revisão a especialistas na mesma área. Seu objetivo é expor um conceito, resolver um problema ou revelar uma descoberta. A ideologia não tem lugar. Além disso, a lista na qual Satoshi postou o “White Paper” era composta por especialistas em matemática, estatística e criptografia que queriam os fatos técnicos simples, não a política que os cercava. Os membros, sem dúvida, tinham uma variedade de pontos de vista políticos, e poderiam muito bem ter tropeçado em alguns com os quais discordavam. A Lista não era o momento, não era o lugar para declarar motivos ou crenças políticas.

No entanto, uma referência política está em posição de destaque. Nota de Rodapé [1] lê, “W. Dai, ‘b-money’, http://www.weidai.com/bmoney.txt, 1998.” Este é o aceno de agradecimento de Satoshi à proposta de b-money de 1998 desenvolvida pelo famoso cypherpunk Wei Dai, com quem Satoshi teve uma troca de e-mails. A proposta de Dai é amplamente vista como uma precursora do “White Paper”, com algumas pessoas acreditando que Dai é Satoshi. Em 22 de Agosto de

2007, Satoshi enviou um e-mail para Dai para o informar, “Estou ficando pronto para lançar um documento que expande suas ideias em um sistema operacional completo”. O fato de os pontos de vista de Dai serem um trampolim para o “White Paper” faz com que valha a pena examiná-los.

A proposta do b-money de Dai começa:

> Sou fascinado pela criptoanarquia de Tim May. Ao contrário das comunidades tradicionalmente associadas à palavra “anarquia”, em uma criptoanarquia o governo não é destruído temporariamente, mas permanentemente proibido e permanentemente desnecessário. É uma comunidade onde a ameaça de violência é impotente porque a violência é impossível, e a violência é impossível porque seus participantes não podem ser vinculados a seus nomes verdadeiros ou locais físicos." A proposta conclui: “O protocolo proposto neste artigo permite que entidades pseudônimas não rastreáveis cooperem umas com as outras de forma mais eficiente, fornecendo-lhes um meio de troca e um método de execução de contratos. Espero que este seja um passo para tornar a criptoanarquia uma possibilidade prática e teórica.

Também é razoável examinar os recursos que Satoshi escolheu incorporar no Bitcoin como um reflexo de sua política. Os recursos incluem

- Descentralização Radical. A primeira linha do resumo do “White Paper” afirma, “uma versão puramente peer-to-peer de dinheiro eletrônico poderia permitir pagamentos online serem enviados diretamente de uma parte para outra sem passar por uma instituição financeira”. Sem líderes, sem burocracia, sem posição de poder além do que o indivíduo exerce sobre si mesmo.
- Privacidade. A Seção 10 do “White Paper” é intitulada “Privacidade”. Ainda que não perfeito, o anonimato buscado e oferecido pelo Bitcoin é muito superior àquele de outras formas de pagamento online. A Seção 10 termina com uma advertência e, talvez, uma indicação de uma melhoria que Satoshi estava planejando

fazer para a Blockchain. "Como um firewall adicional, um novo par de chaves deveria ser usado para cada transação para impedi-las de serem ligadas a um dono comum. Algumas ligações são ainda inevitáveis com transações multi-entradas, as quais necessariamente revelam que suas entradas eram possuídas pelo mesmo dono. O risco é que, se o proprietário de uma chave for revelado, a vinculação poderá revelar outras transações que pertenciam ao mesmo proprietário."

- Pró-capitalismo. O "White Paper" enfatiza as vantagens do Bitcoin para o comércio e para os comerciantes como um sistema de pagamento de empresas livres. Ele afirma: "Com a possibilidade de reversão [que o Bitcoin não acomoda], há a necessidade da confiança se espalhar. Os comerciantes devem ser cautelosos com seus clientes, incomodando-os por mais informações do que eles precisariam". É difícil imaginar um socialista tendo essa percepção ou se importando com os comerciantes.
- Anti-bancos. Todo o propósito do Bitcoin consiste em "pagamentos online […] sem passar por uma instituição financeira." No nono fórum PGP, Satoshi explicou: "A raiz do problema com a moeda convencional é toda a confiança necessária para fazê-la funcionar. O banco central deve ser confiável para não desvalorizar a moeda, mas a história das moedas fiduciárias está cheia de violações dessa confiança. Os bancos devem ser confiáveis para manter nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com meramente uma fração de reserva. Temos que confiar neles nossa privacidade, confiar neles para não deixar ladrões de identidade drenarem nossas contas."
- Antigoverno. Embora o governo não seja mencionado no "White Paper", o Bitcoin é um ataque direto a uma função estatal supostamente vital – o setor bancário. A mensagem no bloco do Genesis foi um tapa no Chancellor tanto quanto no resgate a bancos.
- Anti-inflação. A seção 6 do "White Paper", intitulada "Incentive", afirma que "uma vez que um número predeterminado de moedas tenha entrado em circulação, o incentivo pode fazer a transição inteiramente para taxas de transação e ser completamente livre de inflação". O número predeterminado é de 21 milhões de moedas, cada uma divisível até uma pequena fração de uma moeda inteira.

As características anteriores se aproximam de uma declaração de anarquismo econômico. Um artigo do *CoinJournal* intitulado "Op-Ed: Satoshi Nakamoto is Clearly an Anarchist" refere-se a uma apresentação de 2014 de Daniel Krawisz do Satoshi Nakamoto Institute. Krawisz afirma: "Alguém que promove bitcoin e que não é anarquista é um criptoanarquista porque o bitcoin é inerentemente anarquista."

Evidência a partir de postagens e associações pessoais

As postagens menos formais de Satoshi em fóruns são mais uma evidência de sua política. Novamente, as observações são antibancárias e antigovernamentais, enquanto reconhecem abertamente o apelo do Bitcoin aos libertários.

- Anti-bancos. Novamente, Satoshi escreve: "Os bancos devem ser confiáveis para manter nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com meramente uma fração em reserva."
- Antigoverno: Quando um usuário se opõe ao Bitcoin, dizendo: "Você não encontrará uma solução para os problemas políticos na criptografia", Satoshi responde: "Sim, mas podemos vencer uma grande batalha na corrida armamentista e ganhar um novo território de liberdade por vários anos. Os governos são bons em cortar as cabeças de redes controladas centralmente como o Napster, mas redes P2P puras como Gnutella e Tor parecem estar se mantendo."
- Pró-liberdade. "[Bitcoin é] muito atraente para o ponto de vista libertário se pudermos explicá-lo adequadamente. Eu sou melhor com código do que com palavras". Além disso, a postagem de Satoshi no fórum bitcointalk, O Bitcoin NÃO viola o Teorema da Regressão de Mises, indica sua familiaridade com Mises, e o tópico em si discute o livro-assinatura de Rothbard *Homem, Economia e Estado*.

Associações pessoais são outro indicador de crenças pessoais. O principal entre os associados de Satoshi era o falecido Hal Finney. Desenvolvedor da PGP Corporation, Finney foi o primeiro destinatário de uma transação de bitcoin, que Satoshi enviou a ele em 12 de janeiro de

2009. Finney obviamente cooperou de perto com Satoshi – alguns acreditam que *ele* era Satoshi – o que torna as opiniões políticas de Finney relevantes. No início dos anos 1990, Finney contribuiu regularmente para o listserv dos cypherpunks. Satoshi também postou um link para seu "White Paper" no site cypherpunk da P2P Foundation, onde ele era um membro da lista. Em um post, Finney afirma, "Naturalmente, na sociedade de hoje, com o poder alocado de forma tão desproporcional, essas ideias [criptografia] são uma ameaça para grandes organizações. O poder sendo balanceado significaria uma perda líquida de poder para eles. Portanto, nenhuma instituição vai pegar e defender as ideias de Chaum. Terá que ser uma atividade de base, na qual os indivíduos primeiro aprendam quanto poder eles podem ter e depois o exijam."

Martti Malmi fornece outra pista. Malmi era um estudante da Universidade de Tecnologia de Helsinki, que se tornou um entusiasta do Bitcoin. O livro de Nathaniel Popper *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* descreve a jornada de Malmi. Postando no fórum anti-state.org, que explorou o anarquismo de livre mercado, Malmi escreve sobre o Bitcoin: "Estou realmente empolgado com a ideia de algo prático que possa realmente nos aproximar da liberdade em nossa vida. :-)". Em um e-mail a Satoshi, Malmi incluiu um link para esse post.

Satoshi responde, "Seu entendimento do Bitcoin está certíssimo."

Novamente, Satoshi percebeu totalmente o quão revolucionário seu sistema seria. Quando o Wikileaks permitiu doações de bitcoin como um modo de desviar de um bloqueio financeiro, o Bitcoin foi propulsionado a um novo nível de atenção e popularidade. Um chocado Satoshi postou: "Teria sido bom chamar essa atenção em qualquer outro contexto. O WikiLeaks chutou a colmeia das vespas, e o enxame veio em direção a nós." Ele pediu ao Wikileaks que não destacasse o Bitcoin porque o projeto era jovem o suficiente para ser destruído pelo governo. De fato, a decisão de Satoshi de permanecer anônimo aponta para sua compreensão do perigo envolvido com o Bitcoin. Afinal, os criadores anteriores de dinheiro digital foram processados com destaque, e Satoshi deve ter observado de perto como os processos se desenrolaram.

O argumento anterior não é uma prova definitiva de que Satoshi era um libertário ou um anarquista, mas chega perto disso. "Libertário, anarquista ou ambos" tornam-se a resposta mais plausível *de longe* à pergunta sobre suas crenças políticas.

Evidência do ambiente de Satoshi

A atmosfera político-econômica da qual o Bitcoin emergiu fornece mais uma indicação das crenças de Satoshi. A codificação do Bitcoin começou em 2007, e é improvável que o momento seja uma coincidência. A crise financeira de 2007-2008 foi considerada a pior desde a Grande Depressão da década de 1930. Foi causado em grande parte pelas terceiras partes confiáveis que Satoshi mais se opunha: governos e bancos.

O que aconteceu? Em termos simplistas, a indústria de empréstimos imobiliários de alto risco entrou em colapso e provocou a crise. Um empréstimo imobiliário de alto risco é normalmente emitido para um mutuário com crédito ruim que apresenta um alto risco de inadimplência. Para compensar o credor por esse risco, o mutuário paga uma alta taxa de juros. Os empréstimos imobiliários de alto risco tornaram-se cada vez mais comuns no período anterior a 2007 por várias razões. Um foi o uso de software de subscrição automatizado que acelerou o processo de empréstimo, mas ignorou a revisão padrão de dados e documentos. Em suma, as instituições de crédito não autenticaram a elegibilidade do mutuário. Os preços da habitação dispararam devido a uma enxurrada de crédito artificialmente solto. Atingindo o pico em 2006, os preços iniciaram uma espiral descendente que durou anos e causou execuções massivas tanto nos EUA quanto internacionalmente.

A alta taxa de inadimplência levou a uma desvalorização dos instrumentos financeiros, o que ameaçou o colapso do confiável sistema de terceiros – também conhecido como sistema financeiro. O Estado não iria e não poderia permitir que isso acontecesse; o sistema financeiro era seu braço direito. Em 7 de setembro de 2008, o governo federal dos EUA assumiu as responsabilidades dos extremamente abalados Freddie Mac e Fannie Mae. Outros resgates se seguiram. Em 3 de outubro, a Lei de Estabilização Econômica de Emergência de 2008 autorizou gastos de até US$ 700 bilhões para comprar ativos em dificuldades e financiar instituições financeiras, inclusive estrangeiras. O custo de salvar a hierarquia de terceiras partes confiáveis foi repassado aos pagadores de impostos, é claro.

Satoshi observou os resgates se desenrolarem, como atesta a mensagem de bloqueio do Genesis. A pilhagem de fundos de impostos para enriquecer a elite, enquanto as pessoas comuns perderam suas casas, deve ter parecido um pesadelo de terceiras partes confiáveis.

Outra coisa ocorreu em 2007. O governo federal dos EUA acusou os chefes da e-gold, Inc. de lavagem de dinheiro e transmissão de dinheiro sem licença. Os donos do e-gold foram julgados e condenados; a empresa arruinada foi forçada a fechar suas portas eletrônicas. Satoshi deve ter visto essa situação bem de perto. Ele aprendeu disso. O anonimato era segurança.

Legado de Satoshi

Satoshi produziu uma tecnologia elegante e original que rivaliza com a impressora de Gutenberg em sua importância para o progresso humano porque permite fácil liberdade econômica em nível individual.

O paralelo merece expansão. Embora sua impressora não tenha sido a primeira, Johannes Gutenberg foi pioneiro em inovações criativas que tiveram um impacto semelhante à criação de Satoshi. Ele substituiu as tintas à base de água de curta duração por uma durável à base de óleo, por exemplo. Mais importante ainda, ele usou uma forte liga para criar cerca de 300 bits de tipos separados que poderiam ser rapidamente montados em modelos uniformes e desmontados. As impressoras anteriores usavam pedaços de madeira frágeis ou esculpiam as letras de cada página em um bloco de madeira que era pintado. As inovações transformaram a imprensa de uma ferramenta das classes de elite – a corte, o clero – em uma ferramenta do povo. Gutenberg abriu um mundo de informações e ideias para pessoas comuns que não precisavam mais confiar nas autoridades para sua versão da verdade. A imprensa descentralizou o conhecimento nas mãos do homem comum, e conhecimento é poder. Isso tornou a imprensa não apenas uma maravilha técnica, mas também um agente de mudança e revolução social.

Os que estão no poder teriam evitado a mudança, se pudessem, suprimindo a enxurrada de opiniões e ideias. Um público iletrado, não informado, é mais fácil de controlar. Um público letrado e informado encoraja a ascensão do populismo e de reformadores que ameaçam o status quo. Preservar um status quo favorável ao poder é a principal razão pela qual a censura estatal existia então e agora, sendo o controle da imprensa um fator essencial. Infelizmente para os poderosos, a literatura aumentou e mais pessoas puderam julgar por si mesmas quais crenças religiosas e políticas ressoavam dentro delas como reais.

Um exemplo de convulsão social: sem a imprensa de Gutenberg, a Reforma Protestante provavelmente não teria ocorrido, ou teria sido

muito limitada em escopo. Martinho Lutero lançou a Reforma em 1517 pregando suas noventa e cinco teses na porta de uma igreja alemã. O documento foi rapidamente traduzido do latim para o alemão, depois copiado e reimpresso; no jargão de hoje, tornou-se viral. Como homem, Lutero só podia alcançar aquelas pessoas dentro do alcance de sua voz e caneta. Como um autor produzido em massa, Lutero espalhou ideias por toda a Europa em poucos meses. Em três anos, centenas de milhares de cópias de suas Teses foram produzidas em centenas de prensas tipográficas. A Igreja Católica respondeu excomungando Lutero, levando-o a fugir e a se esconder. As ideias, entretanto, não respondem a ameaças de fogo do inferno, nem fogem.

A imprensa de Gutenberg provocou movimentos e revoluções. Mas a imprensa em si não era ideológica, pois qualquer ideia podia ser montada em moldes e impressa em massa: Catolicismo ou Protestantismo, individualismo ou socialismo, Karl Marx ou Ayn Rand. A máquina ela mesma era neutra. A prensa teve fortes implicações ideológicas, com certeza, porque deu poder ao indivíduo e às massas. Em outras palavras ela era uma forma populista. Mas as autoridades também usaram a nova tecnologia para seus próprios fins estatistas. Por mais magnífica que fosse a imprensa, era uma ferramenta para o bem ou para o mal, dependendo da finalidade do usuário individual.

O mesmo pode ser dito da cripto. Seu empoderamento do indivíduo é um ato profundamente político. Mas esse empoderamento faz todos serem mais livres para escolher quaisquer ideologias que eles queiram. A própria cripto não possui posição ideológica estabelecida. É por isso que individualistas, anarquistas, socialistas, estatistas e entre outros podem usar a blockchain como um modo de perseguir seus fins, independentemente de quais fins esses possam ser. Amir Taaki, um desenvolvedor da Darkmarket? Openbazaar e da Dark Wallet, é um anarquista de esquerda agressivo que passou um tempo em Rojava [Kurdistão Sírio], ajudando a fundar uma República Popular através da introdução do Bitcoin. Rojava estava “sob embargo, então não havia maneira de mover dinheiro para dentro ou para fora”, ele explica. “Então temos realmente de criar nossas próprias economias em bitcoin. Agora temos uma ferramenta tecnológica para as pessoas livremente se organizarem fora [do] sistema do estado. Porque é uma moeda não controlada por bancos centrais.”

O Bitcoin pode atingir uma diversidade galopante de objetivos. Essa é uma grande força. A prensa de Gutenberg providenciou informação e perspectivas que permitiram as pessoas escolherem religião e políticas *por elas mesmas*. A cripto dá às pessoas o controle de seu próprio futuro econômico que lhes permite escolher seus próprios estilos de vida e compromissos. Parte do que faz a Revolução Satoshi brilhar é que ela é profundamente política ao empoderar o indivíduo, mas não exige uma posição ideológica. Ou seja, não diz aos indivíduos empoderados o que eles devem escolher ou como eles podem usar seu próprio poder. A maioria das pessoas veem pouca diferença entre o político e o ideológico. Geralmente não há. Mas às vezes a política e a ideologia são distintas.

O Bitcoin é político no mesmo sentido em que a prensa de Gutemberg. Ela descentraliza o controle até o nível do indivíduo – a cripto é puro empoderamento – mas ela não dita o que indivíduos fazem com seu autocontrole. Isso seria uma contradição em termos. Ainda sim é isso que o estado faz quando ele tenta controlar a cripto; ele tenta vincular uma contradição em termos com a sociedade. O estado toma uma dinâmica inerentemente descentralizada e individualista e tenta centralizá-la ao torná-la um braço do governo. As boas notícias: as tentativas do estado parecem fadadas ao fracasso. A má notícia: o estado continuará tentando.

O Governo Leva a Cripto a Sério

O melhor status para se ter vis-à-vis ao estado, no final das contas, é nenhum – isto é, passar despercebido enquanto você vive sua vida em paz e em liberdade. A invisibilidade é, entretanto, um status difícil ou caro de se alcançar, e o governo pune punições rígidas àqueles que tentam sem sucesso. A cripto perdeu a invisibilidade legal que inicialmente gozou de ser arcana ou desconsiderada como uma faísca numa panela. Está sendo tomada seriamente e é "vista" pelas autoridades. Chamar a atenção do estado é provavelmente o que Satoshi quis dizer quando lamentou a proeminência que o Bitcoin alcançou por meio de sua associação com o Wikileaks. A tecnologia era jovem e estava em desenvolvimento inicial; a última coisa que precisava era ser levada a sério pelo governo. Como Satoshi comentou, "A WikiLeaks chutou o ninho de vespas, e o enxame está vindo em nossa direção."

O objetivo do enxame do estado é previsível – controle –, mas a reação das autoridades varia. Alguns políticos e burocratas percebem uma ameaça; outros vislumbram a mais nova pilhagem possível; outros ainda veem um meio de atualizar um sistema bancário central ineficiente e impopular; muitos querem usá-lo como trampolim para uma sociedade sem dinheiro que eles controlam digitalmente. Quaisquer que sejam as diferenças de perspectiva, no entanto, a mesma conclusão é alcançada: a criptografia precisa estar sob sua autoridade centralizada.

Uma estratégia do estado para controlar a cripto

Uma estratégia popular de estado para dominar cripto é reclassificá-lo como dinheiro e aplicar as mesmas leis rigorosas que cobrem a fiat. Um projeto de lei atualmente parado no Senado dos Estados Unidos incorpora aspectos comuns dessa tática, que está longe de se limitar às costas americanas. Examinar o projeto de lei é uma maneira de entender como essa estratégia provavelmente funcionará e como o processo destruiria as criptomoedas, caso bem-sucedido.

Na terça-feira, 28 de novembro de 2017, o Projeto de lei 1241 do Senado foi ouvido pela Comissão de Justiça do Congresso. O projeto de lei foi discutido no comitê onde ele permanece. É um alarme soando à noite.

Alguns entusiastas das criptos vão aplaudir esse desenvolvimento porque acreditam que a regulamentação significa que a cripto está se tornando mainstream e alcançando uma respeitabilidade que traz mais lucro. Alguns entre aqueles que aplaudem querem se beneficiar de licenças (aprovações governamentais), o que poderia eliminar os concorrentes de livre mercado. Outros fanáticos por criptomoedas apenas irão cruzar os braços porque pensam que as criptomoedas de livre mercado não podem ser controladas e os esforços estatistas falharão. Os indiferentes podem estar corretos – espero que estejam –, mas vidas podem ser destruídas pela tentativa do estado de dominar, e a destruição de pessoas boas é um assunto de não se cruzar os braços. A abordagem prudente à intrusão do estado não é nem o aplauso, nem a indiferença, mas preparação. O governo está chegando e ele quer mais que dinheiro. Ele quer dar exemplos contundentes de usuários de cripto para dissuadir outros de buscar a liberdade financeira.

A "Lei de Combate à Lavagem de Dinheiro, Financiamento do Terrorismo e Falsificação" (S.1241) é um projeto de lei contra a lavagem de dinheiro que regula a criptomoeda a nível federal. Isso significa que haveria uma uniformidade no status legal e no tratamento das criptomoedas em toda a América.

Novamente, alguns entusiastas de criptomoedas aplaudirão esse movimento por fornecer clareza à situação. Essa é uma resposta enganosa em vários níveis. Por um lado, controle não é clareza; é a centralização e a entrega da escolha. E a clareza não tem valor intrínseco à parte do conteúdo que está sendo esclarecido; um assassino pode ser muito claro sobre como ele pretende matar você, mas isso não é algo para comemorar ou buscar. Por outro lado, se inconsistências legais no tratamento das criptos causarem problemas, então a resposta apropriada é remover as leis, não exigir mais.

Além disso, inconsistências na lei podem ser úteis porque podem funcionar para a vantagem daqueles que buscam a liberdade. A estratégia é às vezes chamada de abordagem da "instituição paralela". Instituições paralelas como a Igreja e o Estado podem atuar como baluartes contra o poder um do outro, permitindo que os indivíduos respirem mais profundamente na divisão. O conceito de santuário da igreja estava tradicionalmente disponível para criminosos e escravos fugitivos, por exemplo, embora não fosse oferecido de forma confiável. Por outro

lado, pessoas com crenças religiosas ou políticas "erradas" às vezes podem escapar da perseguição fugindo para o santuário de uma área politicamente mais amigável.

A estratégia da instituição paralela é empregada todos os dias em todo o mundo. Na América, as pessoas se mudam de estados com altos impostos para estados com poucos ou nenhum imposto. Os ricos britânicos se mudam para paraísos fiscais. Os aficionados da maconha se mudam do Texas, com suas leis draconianas sobre drogas, para o Colorado, onde a maconha é legal. Em todo o mundo, as pessoas fogem por suas próprias razões.

A liberdade não se beneficia da homogeneização da lei governamental, mas da presença de alternativas. A federalização da lei sobre criptomoedas para eliminar a inconsistência também elimina a capacidade dos usuários de se mudarem para qualquer jurisdição estadual que seja mais favorável ao seu propósito. A federalização da lei também expande o governo para áreas que ainda não são abordadas no nível estadual; isso inclui controle de fronteira e alfândega. A consistência pode trazer clareza, mas ela não traz escolha. Outra palavra para consistência na lei é a palavra "centralização".

O que é a S.1241?

S.1241 foi introduzido no Comitê do Senado secretamente. Um bitcoiner atencioso notou que a reunião do Judiciário do Senado havia sido listada na página oficial às 10h do dia 28 – o mesmo dia da audiência – depois de ser adicionada à página da Audiência às 18h. na noite anterior. Essa manobra efetivamente impediu a cobertura da mídia, feedback do público ou protestos. Ações para controlar a cripto são prováveis de seguir esse padrão – abrupto, invisível e inesperado. A S.1241 pode ser vista como um modelo de como os governos pretendem proceder. Para onde os EUA vão, grande parte do mundo vai.

A S.1241 procura emendar o Código 31 § 5312, que trata das definições e sua aplicação a dinheiro e finanças. Parece seco, mas o impacto seria dramático. O objetivo do projeto de lei é incluir "moedas digitais" na definição de "instrumentos monetários" e incluir "qualquer corretora digital ou trocador de moeda digital" na definição de "instituição financeira". $10.000 é o valor acionante da lei. Nos EUA. $10.000 aciona uma declaração pessoal na margem; é o ponto em que as instituições financeiras completam um relatório de moeda exigido

pelo estado que pode fazer com que as contas sejam congeladas ou confiscadas, independentemente de haver evidência de um crime

A S.1241 é uma corda apertada

Seção 2: "Transporte ou Transbordo de Cheques em Branco ao Portador" declara que qualquer cheque entrando ou saindo dos EUA que seja "extraído em uma conta contendo mais de US$ 10.000" e não tenha um valor em dólar especificado é "valorizado acima de US$ 10.000 para fins de relatório". Visto que a cripto pode ser difícil de se ensaiar e raramente tem um valor em dólar especificado, o "valor sem dólar" permite que os agentes alfandegários avaliem a cripto no valor registrável.

Seção 3: "Aumentar as penalidades para o contrabando de dinheiro a granel" aborda a ocultação de $10.000 ou mais em moeda ou instrumentos monetários ao cruzar a fronteira. A pena máxima é de dez anos de prisão com multas aumentando em um valor não especificado. Quando o estado pune uma pequena ofensa de maneira draconiana, isso significa que as autoridades não têm outra solução para a situação senão o cano de um fuzil.

Seção 4: A "Seção 1957 Violação Envolvendo Fundos Combinados e Transações Agregadas" trata da "transferência de produtos criminais [...] Sem a necessidade de demonstrar" intenção criminosa. Duas brechas existentes seriam fechadas. 1) $10.000 em fundos nos quais dinheiro supostamente sujo é misturado com dinheiro limpo tornam-se $10.000 de dinheiro sujo. 2) Uma série de transações abaixo de $10.000 que estão "intimamente relacionadas no tempo, a identidade das partes, a natureza das transações ou a maneira como são conduzidas" atendem coletivamente ao limite de $10.000. O dinheiro legal que está na presença de dinheiro "criminoso" é culpado por cumplicidade, permitindo que os funcionários confisquem tudo. Cripto não declarada ou declarada incorretamente torna toda a riqueza – seja cripto ou não – um alvo fácil.

Seção 5: "Acusação de lavagem de dinheiro como um curso de conduta" simplifica o processo de acusação de uma pessoa por lavagem de dinheiro e inclui "conspirações para violar [...] [a] proibição das empresas que transmitem dinheiro não licenciado são rotuladas enquanto conspirações de lavagem de dinheiro". Planos de transmissão de cripto podem ser punidos como se o ato tivesse ocorrido. Não está claro se os

co-conspiradores também serão acusados ou terão seu dinheiro confiscado.

Seção 6: “Empresas de serviços financeiros ilegais” torna crime para empresas não registradas enviar “receitas para o exterior”. O desconhecimento da necessidade de registro não é defesa. O termo “negócio de transmissão de dinheiro” é substituído por “negócio de serviços monetários” para incluir “entidades [...] como caixas de cheques” que “não transmitem dinheiro”. As penalidades e multas aumentam.

Seção 7: “Lavagem de dinheiro oculta” aplica-se a “entregadores ou mulas”. A Suprema Corte decidiu no passado que um réu precisa saber que o transporte de fundos é clandestino e porque os fundos estão sendo “transportados” para que um entregador seja culpado de um crime. Esses requisitos são diluídos ou eliminados. Novamente, ignorância não é uma defesa.

Seção 8 “Congelamento de contas bancárias de pessoas presas pela movimentação de dinheiro através das fronteiras internacionais”. Uma retenção de 30 dias é instituída nas contas dos acusados e pode ser estendida “por uma boa causa”. Isso parece se aplicar ao valor total de uma conta.

Seção 9: “Proibir a lavagem de dinheiro por meio de Hawalas, outros sistemas informais de transferência de valor e transações estreitamente relacionadas” redefine o que constitui um crime de lavagem de dinheiro quando envolve “um conjunto de transações paralelas ou dependentes”. Todos seriam considerados “um único plano ou arranjo”, o que poderia levar a transação coletiva a níveis passíveis de ação judicial.

Seção 10: “Restaurar a autoridade de escutas telefônicas para certas infrações de lavagem de dinheiro e falsificação” permite que o estado monitore as pessoas suspeitas de atividade criminosa.

Seção 11: “Aplicando o Estatuto Internacional de Lavagem de Dinheiro à Evasão Fiscal” define o uso de contas estrangeiras para sonegação de impostos como lavagem de dinheiro. Como a cripto flui tão facilmente através das fronteiras, os usuários tendem a frequentar corretoras “estrangeiras” – uma prática que pode ser rotulada de “evasão fiscal”, a menos que se prove o contrário.

Seção 12: “Conduta em auxílio à falsificação” inclui o uso de novas tecnologias, “materiais, ferramentas ou maquinário”. Esta disposição visa especificamente a criptomoeda, o dinheiro digital e as ferramentas que fornecem privacidade a eles.

Seção 13: “Dispositivos de acesso pré-pago, cartões de valor armazenado, moedas digitais e outros instrumentos semelhantes” altera a lei atual para incluir explicitamente “qualquer corretora digital ou tumbler de moeda digital”, bem como qualquer “emissor, resgatador ou caixa” de uma “moeda digital”. Os fundos armazenados em formato digital estão explicitamente sujeitos a requisitos de relatórios de lavagem de dinheiro.

Seção 14: “Intimações Administrativas para Casos de Lavagem de Dinheiro” expande a disponibilidade e facilidade de intimações administrativas.

Seção 15: “Obtenção de Registros Bancários Estrangeiros de Bancos com os EUA. Contas Correspondentes” fortalece “essa ferramenta de investigação existente”. Bancos estrangeiros podem ser intimados para registros relacionados a qualquer “ação de confisco civil” e podem ser punidos por descumprimento. Relembre-se: A S.1241 inclui “qualquer cambiador digital ou tumbler moeda digital” na definição de “instituição financeira”, o que deixa as moedas estrangeiras vulneráveis a intimações.

Seção 16: “Danger Pay Allowance” fornece compensação especial para uma ampla gama de agências de aplicação da lei. Não está claro o que constitui “perigo”, mas, presumivelmente, as agências terão interesse em definir situações de uma maneira que atraia mais financiamento.

Seção 17: “Esclarecimento da Autoridade do Serviço Secreto para Investigar Lavagem de Dinheiro” expande a autoridade policial.

Seção 18: A “Proibição de Ocultação de Titularidade de Conta” torna crime que uma pessoa “oculte, falsifique ou deturpe conscientemente, de ou para uma instituição financeira” sua identidade ou “fato relativo à propriedade ou controle de uma conta ou ativos mantidos em uma conta.” Isso é particularmente relevante para usuários de cripto que rotineiramente empregam anonimato ou pseudonimato. Torna-se um crime não revelar identidades ou transferências específicas na blockchain.

Seção 19: A “Proibição de Ocultação de Fonte de Ativos em Transações Monetárias” permite que o governo busque ativos mesmo que a pessoa não seja acusada de um crime. Em vez disso, seu dinheiro pode ser confiscado simplesmente porque sua fonte não é declarada ou não é manifesta.

O advogado Ballard Spahr explica: “Se aprovado em sua forma atual, a S.1241 ironicamente levará ao único tipo de ofensa que o Congresso historicamente não tem permitido, construir um pretexto na aplicação das leis de lavagem de dinheiro – ou seja, tratar como tal a fraude fiscal “comum”, que não envolve receitas ilegais – e virar as coisas de cabeça para baixo. Ou seja, as transações que promovam um crime fiscal, desde que envolvam uma transação transfronteiriça, serão o único tipo de transação que pode constituir um crime de lavagem de capitais quando os rendimentos representarem fundos inteiramente legais.”

Aqueles que desejam se preparar contra a repressão vindoura devem estudar a S.1241.

Protegendo as pessoas de sua liberdade

Lavagem de dinheiro e evasão fiscal são duas justificativas que o estado proclama quando tenta controlar as criptos. Indiscutivelmente, essas justificativas amplas e vagas não são vistas com simpatia geral, porque muitas vezes parecem um flagrante roubo monetário.

Outras justificativas são mais bem-sucedidas. A comunidade cripto, argumenta o governo, está repleta de traficantes de drogas, chantagistas, traficantes de sexo, produtores de pornografia infantil, traficantes de armas e outros malfeitores. O estado aponta a “dark web” como prova dessa perfídia. Esta é a parte da web que é acessada apenas por software especial, permitindo que os usuários permaneçam anônimos ou não rastreáveis. Diz-se que o controle de criptomoedas é necessário para proteger as pessoas do crime na dark web. Ao fazê-lo, o estado argumenta que está protegendo usuários de drogas vulneráveis, mulheres e crianças exploradas, vítimas de armas, pagadores de impostos obedientes, cidadãos cumpridores da lei e uma lista de outras “vítimas” dos bandidos monetários.

Existem inúmeras maneiras de refutar essa afirmação, incluindo o fato de que ela é totalmente falsa. Alguns usuários de cripto são, sem dúvida, criminosos violentos; o mesmo acontece com algumas pessoas que usam dinheiro e cartões de crédito. Criptos são moedas e métodos de pagamento. Como qualquer outra coisa útil na vida, é uma ferramenta que pode ser empregada para bons ou maus propósitos. Mas a esmagadora maioria das pessoas com cripto ou com dinheiro são seres humanos pacíficos que estão sendo criminalizados por preferir um método de pagamento em detrimento de outro. A justificativa para isso se

resume à alegação de que suas escolhas econômicas são perigosas para o bem-estar público.

Reprimir práticas econômicas supostamente exploradoras, mas não violentas, é uma tremenda violação dos direitos das pessoas vulneráveis; não os protege. Eu sei. Minha vida poderia ter sido arruinada por uma medida destinada a evitar a assim chamada forma de exploração econômica que repugna à maioria das pessoas – o trabalho infantil. Aos 16 anos, fugi de casa e morei na rua o menor tempo que pude. Recuseime a ir para um abrigo ou procurar ajuda do governo pelo mesmo motivo que muitos adolescentes fugitivos; quando os adolescentes preferem o relento à casa, significa que os adultos os traíram. A única segurança é cuidar de si mesmo.

Eu tive mais sorte do que muitos. Eu mal tinha 16 anos, mas isso significava que eu poderia trabalhar legalmente. Eu poderia ficar atrás do balcão quente em um restaurante de fast food ou, no meu caso, poderia sentar-me no escritório de uma loja de móveis de propriedade familiar, onde eu fazia anos de papelada durante o dia e dormia em um sofá no andar de baixo durante a noite. O dono me pagava um salário-mínimo e me dava um lugar seguro para dormir. Como resultado, trabalhei muito mais do que as oito horas diárias pelas quais fui paga. Economizei o suficiente para me mudar para uma pensão e, quando passei para um trabalho de arquivamento em um banco, tive uma referência. Meu futuro dependia de ter essas oportunidades.

E se eu fosse um mês ou um ano mais nova do que a idade legal para trabalhar? O dono da loja não teria arriscado seu negócio me contratando. Nem deveria. Ele estava certo em insistir em inspecionar e xerocar minha identidade. antes de me oferecer o emprego; ele estava certo em esperar até me conhecer um pouco melhor para me oferecer o sofá do porão. Por que ele deveria colocar a renda e o futuro de sua família em perigo para ajudar uma estranha? E foi isso o que ele fez; ele não me explorou. Ele me *ajudou*.

Sem a capacidade de ganhar dinheiro legalmente, minha vida poderia ter acabado mal em vez de bem. Em nome do humanitarismo, a lei teria trancado minha única porta para a sociedade comum, e teria feito isso segundo seu próprio parâmetro arbitrário de justiça. Como eu teria me alimentado então? Roubo, mendicância, trabalho sexual e tráfico de drogas vêm à mente. Mas eu queria um caminho *para fora* da rua, não uma forma de fazer dela ou da prisão meu endereço permanente.

Fechar opções econômicas não violentas não protege as pessoas vulneráveis. Assim como o aumento do salário-mínimo obrigatório torna difícil encontrar emprego para quem está começando, as "proteções" econômicas impedem que as pessoas vulneráveis possam ascender. No meu caso, não poder me sustentar teria criado uma criminosa e uma vítima, diminuindo o bem público. Se houver violência envolvida em uma opção econômica, então trate a violência. Se não houver, então deixe isso sozinho. Este princípio é a maneira de ajudar a todos que querem ganhar seu próprio dinheiro e gastá-lo como bem entenderem. O estado não protege as vítimas ou a sociedade tirando opções econômicas de pessoas que não causaram danos demonstráveis, mas que por acaso se enquadram em uma categoria que é protegida ou vilipendiada.

Estranhamente, a resposta da lei a ambas as categorias é mais do mesmo: negar direitos econômicos. Como uma adolescente fugitiva, eu estava na categoria "protegida" e quase perdi meu direito de ganhar a vida. Usuários de criptomoedas pacíficos estão na categoria "injuriados", e muitos podem ser destituídos do direito de reter o dinheiro que ganharam.

Para beneficiar os vulneráveis e a sociedade, o estado não precisa fazer nada além de sair do caminho. A frase francesa "laissez faire" é mais frequentemente associada ao "capitalismo laissez-faire". Diz-se que se originou durante uma reunião de 1681 entre Jean-Baptiste Colbert, o Controlador-Geral de Finanças francês, e um grupo de empresários. Colbert perguntou como o Estado poderia ajudar os homens em seus negócios. O chefe do grupo, M. Le Gendre, teria respondido: "laissez nous faire" (deixe conosco). Deixe-nos em paz.

Uma segunda estratégia de controle: Cripto emitida pelo governo

Alguns estados planejam ou tentam emitir sua própria criptomoeda. A moeda digital emitida pelo Banco Central (CBDC) refere-se a uma criptomoeda nacional emitida por um banco central. É a contrapartida cripto de uma moeda fiduciária física, como o dólar americano ou a libra esterlina.

É também uma ironia amarga. Um pulo do gato monetário que foi projetado para minar o sistema financeiro está sendo redefinido para servir ao status quo. Pelo menos, é isso que o status quo espera que aconteça. Para ser justo, alguns líderes mundiais entendem que esse desenvolvimento não é possível. Putin de forma infame disse que uma

criptomoeda nacional não é viável porque a criptomoeda é um fenômeno internacional. Outras nações estão explorando ativamente o desenvolvimento de CBDCs, no entanto. O Japão lançou o dinheiro digital J-Coin, por exemplo. É uma moeda digital em vez de ser uma criptomoeda baseada em blockchain, mas serve ao propósito de aproximar o Japão de uma sociedade sem dinheiro vivo; torna o rastreamento de usuários de moedas digitais uma questão trivial; e permite que o estado reprima usuários de criptomoedas reais com maior facilidade e menos reação. Esses são três dos principais objetivos de uma moeda eletrônica nacional.

As CBDCs podem parecer paralelos à cripto de livre mercado, mas elas são anticripto. Considere apenas algumas das diferenças técnicas:

- Bitcoin é descentralizado; As CBDCs centralizariam todos os aspectos da moeda digital, muitas vezes nas mãos de uma agência ou sistema de agências que são fortemente regulamentadas.
- Bitcoin é peer-to-peer entre indivíduos; CBDCs seriam administradas por terceiras partes confiáveis no pior sentido desse termo.
- Bitcoin é de código aberto; Os CBDCs seriam patenteadas, proprietárias e não transparentes.
- Bitcoin é minerado; CBDCs seriam emitidas por uma autoridade central.
- Bitcoin é limitado a 21 milhões de moedas; O limite das CBDCs seria o que a autoridade desejasse.
- O Bitcoin está em uma blockchain transparente; CBDCs podem não usar uma blockchain, e provavelmente não usariam.
- Os usuários de Bitcoin possuem suas próprias chaves privadas; chaves privadas para CBDCs seriam de propriedade de uma terceira parte confiável que controlaria a riqueza.
- Bitcoin é anônimo; Os CBDCs rastreiam as identidades dos usuários e como eles gastam a moeda.
- O Bitcoin corta a conexão entre a moeda e os bancos centrais; Os CBDCs iriam cimentá-la.

As criptos de livre mercado e as CBDCs também têm objetivos antagônicos. A criptomoeda torna obsoleto o status do banco central como uma terceira parte confiável e elimina o monopólio do dinheiro. As CBDCs são a tentativa do sistema de banco central de manter seu status de terceira parte confiável e o monopólio monetário.

As criptomoedas de livre mercado e as CBDCs podem ter um objetivo em comum, no entanto: a eliminação final do fiat. Mas, novamente, as razões são antagônicas. A cripto rejeita uma moeda corrupta que rouba de pessoas honestas. As CBDCs querem resgatar o status quo em benefício das elites financeiras criando uma fiat digital.

Por que o impulso para uma sociedade sem dinheiro?

O dinheiro congelado sempre foi o inimigo de governo. Em seu artigo "Por que os governos odeiam o dinheiro", o professor de economia Joseph Salerno escreve:

> Agora, a razão dada por nossos governantes para suprimir o dinheiro é manter a sociedade a salvo de terroristas, sonegadores de impostos, lavadores de dinheiro, cartéis de drogas e outros vilões reais ou imaginários. O real objetivo da enchente de leis restringindo ou até proibindo o uso de dinheiro é forçar o povo a fazer pagamentos através do sistema financeiro. Isso permite que os governos expandam sua capacidade de espionar e acompanhar as transações financeiras mais privadas de seus cidadãos, a fim de extrair deles até o último dólar de pagamentos de impostos que eles alegam ser devidos.

O problema que as autoridades enfrentam: Quando o dinheiro sai do banco e vai para os bolsos dos indivíduos, o governo perde a noção de como é gasto. Os indivíduos podem comprar e vender com um anonimato que bloqueia a cobrança de impostos, taxas e outras receitas para o estado. O governo quer "resolver" isso. Sites de rastreamento de dinheiro podem registrar os números de série da moeda fiduciária, por exemplo, e permitir que a circulação seja monitorada, ou seja, desde que o número de série seja reinserido em todas as etapas. O sistema requer um alto grau de cooperação improvável.

O impulso em direção à moeda fiduciária rastreável inevitavelmente falhará devido à falta de cooperação. Felizmente para governos e bancos centrais, o dinheiro digital é um substituto perfeito para o dinheiro físico porque a rastreabilidade é incorporada ao projeto. Se os governos conseguirem fazer o dinheiro digital funcionar, os dinheiros

resultantes serão um pesadelo para a liberdade. Eles combinarão a eficiência das criptomoedas com o totalitarismo do governo. O problema da terceira parte confiável que o Bitcoin foi criado para eliminar estará de volta com esteroides.

A hostilidade do estado ao dinheiro fará com que algumas nações passem da moeda fiduciária física para a digital com entusiasmo. É provável que o processo se pareça com alguma versão do seguinte:

Primeiro: Um governo explora a possibilidade de dinheiro digital enquanto remove gradualmente o dinheiro físico de circulação.

Segundo: Um banco de dados para moeda digital – provavelmente não baseado em uma blockchain – é escrito em código proprietário e implementado de maneira não transparente.

Terceiro: Um dinheiro digital é emitido e vendido como uma alternativa ao dinheiro e à cripto de livre mercado. Para encorajar sua adoção, o governo regula as criptos de livre mercado que são levadas à clandestinidade ou forçadas a fugir para climas mais amigáveis.

Quarto: A tributação automática é embebida na nova moeda digital. O rastreamento absoluto de cada unidade de moeda, que está ligada a identidades reais, dá ao governo um controle sem precedentes sobre o fluxo de riqueza.

Quinto: Bancos centrais inflacionam a oferta de moeda digital à vontade, desvalorizando cada unidade em circulação. Isso inflige um imposto enorme e oculto a todos os proprietários.

A CBDC também dá ao governo maior precisão na manipulação da economia. Em um artigo intitulado "Por que os governos querem uma moeda digital emitida pelo Banco Central", o economista austríaco Xiong Yue observa:

> [D]ado que essas moedas digitais são programáveis, o governo pode até controlar exatamente como gastar esse novo dinheiro usando scripts. Por exemplo, se o governo planeja subsidiar certas fazendas, digamos algumas fazendas de milho, para apoiar este setor da agricultura, eles podem adicionar diretamente uma certa quantia de dinheiro às carteiras de algumas fazendas, por exemplo, 100 milhões de dólares e programar esse dinheiro para ser enviado a certos comerciantes de fertilizantes em um determinado momento, e que cada um só possa gastar no máximo 10 milhões de dólares por ano.

Em suma, uma CBDC poderia facilitar um estado centralizado mais eficiente. Isso dificilmente é uma coisa boa.

Outro item da agenda do governo e dos bancos centrais são as taxas de juros negativas. Os juros negativos ocorrem quando os depositantes não recebem juros sobre o dinheiro mantido em suas contas; em vez disso, eles pagam juros ao banco por reter seu dinheiro. Esse é uma fábrica de dinheiro para os bancos. Também incentiva as pessoas a gastar porque o dinheiro se desgasta se não for gasto, e os gastos do consumidor parecem sustentar a economia.

A crise bancária de 2015 na Grécia é um exemplo de como os juros negativos funcionam. Para evitar corridas bancárias, a Grécia impôs uma sobretaxa de um euro por 1.000 euros em saques em dinheiro. Salerno observa: "Não parece muito grande, mas o *princípio* em ação é extremamente grande porque o que eles estão fazendo é quebrar a taxa de câmbio entre uma unidade de depósitos bancários e uma unidade de moeda." Salerno continua: "Para facilitar os cálculos […] digamos que a 'sobretaxa' grega é de dez dólares para cada 100 dólares sacados. Agora, em vez de poder converter um euro em sua conta corrente em um euro em dinheiro, sob demanda, você só poderá comprar um euro em dinheiro gastando 1,10 euros em suas contas bancárias. Isso é uma taxa negativa de 10% em algum sentido. […] Então, você realmente só receberia noventa centavos para cada dólar que você quisesse sacar e isso é muito significativo pois significa que será mais caro comprar um item com dinheiro do que com depósitos bancários." Previsivelmente, as pessoas foram afastadas do dinheiro. Havia um incentivo para pagar contas domésticas a partir de suas contas bancárias, o que tornava todos os pagamentos rastreáveis.

O principal problema com um esquema de juros negativos para o governo e os bancos centrais é que as pessoas manterão seu dinheiro fora do sistema financeiro. Quantias grandes irão se manter além do alcance do governo. Se, entretanto, o dinheiro digital for totalmente adotado, então o governo pode insistir que as pessoas o usem em vez de dinheiro digital para pagamentos tais como impostos. Isso significa que a riqueza ficará presa no sistema financeiro.

A estratégia das corretoras centralizadas

> A raiz do problema com a moeda convencional é toda a confiança necessária para fazê-la funcionar […] Temos de confiar a elas [terceiras partes] nossa privacidade, confiar que elas não permitam que ladrões de identidade [incluindo o governo] drenem nossas contas.
> – Satoshi Nakamoto

A única coisa a que as CBDCs não podem sobreviver é a competição de livre-mercado. É por isso que todo estado que busca uma CBDC fará um esforço conjunto para eliminar ou aleijar as alternativas de livre mercado. Um aspecto interessante dessa repressão é que existe uma forma de cripto não estatal que a maioria dos governos tolerará: moedas digitais emitidas por instituições financeiras licenciadas. Essas moedas não são um desafio para o sistema bancário central porque as instituições emissoras são regulamentadas para agir como se fossem bancos afiliados. Corretoras licenciadas tornam-se o lobby externo do sistema bancário central. O lobby imita o livre mercado de algumas maneiras, mas não tem nenhuma relação real com ele.

Uma definição padrão de uma corretora centralizada: "As corretoras de criptomoedas centralizadas são plataformas online usadas para comprar e vender criptomoedas. Eles são os meios mais comuns que os investidores usam para comprar e vender reservas em criptomoedas." Uma corretora centralizada é um mercado para negociar ou converter ativos por meio de um único local ou serviço. No entanto, a definição não captura os problemas que as corretoras centralizadas apresentam ao modelo Satoshi.

Mas, primeiro, quais são os problemas que as corretoras centralizadas resolvem? Por que elas vieram a existir? Há uma demanda de mercado para especular, negociar moedas e realizar outras transações financeiras sofisticadas para as quais as estruturas peer-to-peer – corretoras descentralizadas – ainda não estão adequadamente equipadas. Há também uma demanda por conveniência e acesso a cripto que não requer conhecimento técnico ou esforço. Para alguns, as corretoras centralizadas também têm a familiaridade reconfortante dos bancos. Ou elas preenchem um nicho ou então elas não seriam populares. Atualmente, elas dominam grande parte do mundo das criptos, com a maioria dos usuários confiando às corretoras sua riqueza e privacidade.

O nicho ocupado pelas corretoras centralizadas vem da combinação das funções de um mercado de ações com a de um banco. De muitas

maneiras, elas são semelhantes à Bolsa de Valores de Nova York. Moedas podem ser negociadas, vendidas e sacadas por moeda fiduciária, por exemplo; o trading à margem, stop loss e empréstimos também estão disponíveis. De outras maneiras, as corretoras centralizadas se assemelham aos bancos tradicionais. Depois de comprar cripto de uma corretora, muitos clientes escolhem deixar suas moedas em uma conta em vez de transferi-las para suas carteiras privadas em seus próprios discos rígidos. As corretoras centralizadas tornam-se terceiras partes confiáveis; isso significa que elas representam um perigo terrível para a riqueza e o bem-estar dos titulares de contas. Considere um aspecto do risco. A maioria das corretoras centralizadas possuem as chaves privadas dos titulares das contas. Mas as chaves privadas *são* as criptos. As moedas não possuem presença física, apenas algorítmicas. Quando uma corretora controla as chaves, ela de fato é proprietária das moedas. O cliente não tem nada mais do que uma promessa de acesso a elas sob demanda, da mesma forma que os bancos prometem acesso a dinheiro físico mediante solicitação de um titular de conta.

Recentemente, os riscos associados às corretoras centralizadas aumentaram exponencialmente e por um motivo: as corretoras estão cada vez mais cumprindo ou fazendo parceria com o estado para fazer cumprir as leis e os requisitos de relatórios aos clientes. Um artigo da *Forbes* de fevereiro de 2018 anunciou o inevitável em relação à maior corretora centralizada do mundo.

> Finalmente está acontecendo: A movimentada movimentação de documentos na batalha entre o Internal Revenue Service (IRS) e a Coinbase, uma empresa que facilita transações de moedas digitais como Bitcoin e Ethereum, está avançando. A Coinbase anunciou que notificou os clientes afetados de que cumprirá uma ordem judicial em relação à liberação de dados específicos.

2018 foi o ano em que as agências fiscais americanas levaram a sério os lucros e reservas em criptomoedas. Governos de todo o mundo estão observando a Coinbase fornecer dados sobre seus clientes, o que quase certamente levará a auditorias e/ou processos judiciais de alto nível. Especificamente, a Coinbase está relatando todos os clientes com transações de $20.000 ou mais em um único ano entre 2013 e 2015.

Serão entregues identidades, nomes reais, datas de nascimento, endereços e todos os registros de transações. A riqueza de dados está disponível porque a Coinbase, como qualquer outra corretora licenciada, está em conformidade com as leis de Know Your Customer e Anti-Lavagem de Dinheiro que destroem a privacidade financeira.

A Coinbase se tornou extremamente agressiva na coleta de informações e na verificação de identidades. A corretora usa a tecnologia de reconhecimento facial, por exemplo, para comparar uma foto de rosto em tempo real de uma webcam ou smartphone com qualquer documento de identidade enviado pelo candidato. Espere que a intrusão agressiva se torne a norma para trocas centralizadas porque elas valorizam suas licenças e relacionamentos com o governo. Espere que elas atuem como braços de coleta de dados do estado. O perigo não é apenas o congelamento e confisco de contas, mas também os processos judiciais e a prisão dos titulares de contas. O IRS declara que "qualquer pessoa condenada por evasão fiscal está sujeita a uma pena de prisão de até cinco anos e uma multa de até $250.000. Qualquer pessoa condenada por apresentar uma declaração falsa está sujeita a uma pena de prisão de até três anos e multa de até $250.000."

Felizmente, a demanda do mercado para o mercado de ações e por funções bancárias pode ser satisfeita (ou em breve será satisfeita) sem sacrificar a privacidade e a segurança. Uma corretora descentralizada é um mercado que não depende de serviços de terceiros. As negociações são peer-to-peer; são transferências diretas entre pessoas que utilizam um processo automatizado para facilitar a troca. Elas são isentas da necessidade de confiança. Elas são transparentes, com o software e suas transações sendo de código aberto. Elas são Satoshi.

Uma corretora descentralizada permite que os indivíduos mantenham suas próprias chaves privadas, o que a torna um alvo menos atraente para hackers. Também requer uma quantidade mínima de dados pessoais ou financeiros para estabelecer uma conta e realizar comércio. Muitas vezes, apenas um endereço de e-mail é solicitado e pode ser gerado especificamente para registro, sem conexão com uma identidade real.

As corretoras descentralizadas empregam uma ampla variedade de estratégias para facilitar as transferências peer-to-peer. Alguns criam tokens proxy; outros empregam um depósito de múltiplas assinaturas. O banco peer-to-peer usa uma dinâmica do tipo leilão para facilitar em-

préstimos de um valor específico e a uma taxa acordada entre os membros. Os contratos inteligentes podem assumir as funções tradicionais dos bancos. A *Technology Review* explica:

Alternar entre dinheiro fiduciário e criptomoeda exigirá um ponto de troca tradicional no futuro próximo. Mas alguns tecnólogos dizem que é possível um modelo alternativo para negociar criptomoedas que daria às pessoas mais controle sobre sua riqueza. Suas metacorretoras podem ser descentralizadas, eles dizem, usando uma blockchain. A ideia depende especificamente dos chamados contratos inteligentes, código de software que pode ser armazenado em uma blockchain e configurado para controlar as transações programaticamente. Imagine, por exemplo, que você queira enviar a seu amigo alguma criptomoeda automaticamente em uma data e hora específicas. Você pode usar um contrato inteligente para fazer isso.

A questão aqui é *não* defender uma tática de descentralização específica. É oferecer uma noção das alternativas ricas e em evolução às corretoras centralizadas. Muitas pessoas ainda escolherão uma corretora centralizada porque as plataformas são fáceis de acessar e usar; eles são sancionados pelo governo e isso significa respeitabilidade para algumas pessoas; e oferecem as funções familiares e avançadas de um mercado de ações. As pessoas têm todo o direito de fazer essa escolha com seu próprio dinheiro, é claro. Mas para aqueles que valorizam a privacidade, é uma alternativa inaceitável. (Mais sobre corretoras descentralizadas posteriormente).

Uma analogia ilustra a diferença gritante em como a privacidade e os direitos se comportam em um sistema centralizado e descentralizado: mídia social.

"'Quer enlouquecer?' Aqui estão todos os dados pessoais que o Facebook/Google coleta". Esta é uma manchete de março de 2018 em *Zero Hedge*. Os tipos de dados coletados são extensivos demais para enumerar. Um exemplo: Os usuários de celulares Android que baixaram aplicativos específicos do Facebook tiveram dados sobre suas chamadas pessoais registradas pelo Facebook por anos.

Uma causa relativamente não discutida da hemorragia de privacidade das mídias sociais e sua abreviação da liberdade de expressão é a centralização de informações e discussões que acompanham as empresas gigantes, como Facebook e Google. Grandes corporações formam alianças de conveniência e lucro recíproco com o governo. Um artigo intrigante no *The Federalist* pergunta: "As mídias sociais foram um

erro?" O autor, Robert Tracinski, remonta aos anos 2000 – a era de ouro dos blogs, quando todos, até suas avós, se expressaram através de blogs.

Tracinski escreve: "Parecia uma liberação. A era dos blogs ofereceu a promessa de uma mídia descentralizada. Qualquer um poderia publicar e comentar as notícias e encontrar uma audiência. [...] Estávamos ignorando os antigos guardiões da mídia. E tivemos o controle sobre eles! Nós postamos em nossos próprios sites. Tivemos boas discussões sobre nossos campos de comentário, os quais nós moderamos." Era um turbilhão de liberdade de expressão, mas também era um bastião de privacidade porque os indivíduos mantinham o controle. O controle individual de dados e expressão é liberdade.

Então as mídias sociais chegaram como um rolo compressor, e os blogs familiares migraram seus diários e informações para o Facebook, Google, Twitter e outras terceiras partes confiáveis. Assim como as corretoras centralizadas, os gigantes da mídia social eram relativamente fáceis de acessar e usar; eles ofereciam software e funções sofisticadas que os blogueiros individuais não tinham conhecimento técnico ou dinheiro para implementar; as mídias sociais deslizaram perfeitamente para os telefones celulares por meio de aplicativos que pareciam abrir o mundo. Na realidade, eles fecharam a libertação pessoal.

Tracinski observa o resultado.

> Alguns dos melhores e mais interessantes blogs tornaram-se publicações on-line completas, mas muitos dos pequenos, peculiares e amadores blog de uma só pessoa se mudaram para as mídias sociais. Isso se mostrou como um grande erro, porque a era da mídia social *re-centralizou* a mídia. Em vez de um milhão de blogs – o que Glenn Reynolds, famoso pelo Instapundit, chamou de "Exército de Davids" – agora temos uma economia de mídia social controlada principalmente por três grandes empresas: Twitter, Facebook e Google.

O preço de centralizar a escrita pessoal tornou-se aparente. A política esquerdista dos gigantes da mídia social significa que eles purgam (suspenderam contas) ou puniram (contas limitadas) aqueles que têm opiniões "erradas". Isso é semelhante a bancos e outras instituições financeiras que se recusam a lidar com pornografia, maconha ou indús-

trias de armas devido à pressão política do governo. Os “antigos guardiões da mídia” foram substituídos pelos puritanos igualmente intrusivos do Vale do Silício. Embora ambos possam ser preferíveis à intervenção direta do governo, seus quase monopólios são reforçados por privilégios fiscais, por regulamentação favorável e por financiamento de impostos diretos. Em suma, eles podem não ser do governo, mas certamente são comparsas do estado e devem sua lealdade a ele. Como resultado, os indivíduos perderam o controle de seu próprio trabalho e dados. Talvez seja mais correto dizer que eles o abandonaram.

Em nenhum lugar o preço da centralização da expressão pessoal é mais gritante do que com os dados pessoais. Em retorno pela conveniência, tudo o que as mídias sociais pediam era conhecer e comercializar cada detalhe da vida dos clientes. O papel da centralização nesse estupro da privacidade foi fundamental para sua eficácia.

A Privacidade é a linha de frente da defesa da liberdade individual. A descentralização é a condição social sob a qual a privacidade prospera. Ninguém pode ou deve dizer aos indivíduos qual estratégia usar. Mas, se você valoriza privacidade e segurança, mantenha a privacidade e descentralize.

SEÇÃO DOIS

O Imperativo da Privacidade

Quando a Privacidade é Criminalizada, Apenas os Criminosos têm Privacidade

> "Eu cresci entendendo que no mundo em que eu vivia as pessoas desfrutavam de uma espécie de liberdade para se comunicarem umas com as outras em privacidade, sem serem monitoradas, medidas, analisadas ou julgadas por essas figuras e sistemas sombrios que vivem mencionando o tempo todo na mídia."
> – Edward Snowden

Quero a seguinte mensagem escrita em minha lápide: "Eu vivi. Eu morri. Agora cuide da sua maldita vida." O que eu teria a esconder? Tudo! Que é o mesmo que dizer: qualquer informação que eu seja obrigada a revelar são dados que eu me recuso a divulgar.

No entanto, uma questão fundamental paira sobre essa retórica fervorosa e rebelde:

O que é Privacidade?

Uma resposta famosa vem de um artigo dos advogados americanos Samuel Warren e Louis Brandeis, que apareceu em uma edição de 1890 da *Harvard Law Review*. É uma das peças mais influentes na história da teoria jurídica ocidental. "The Right to Privacy" foi chamado de primeiro apelo proeminente para a privacidade como um conceito a ser consolidado na lei.

O artigo começa da seguinte maneira:

> "QUE o indivíduo deve ter plena proteção pessoal e patrimonial é um princípio tão antigo quanto o direito comum; mas foi considerado necessário, de tempos em tempos, definir novamente a natureza exata e a extensão de tal proteção."

Em outros lugares, a privacidade é definida como o direito de ser deixado em paz.

O artigo defende a privacidade como um direito humano "fundamental" ou básico sobre o qual repousam todos os outros direitos. "O direito de propriedade em seu sentido mais amplo, incluindo todos os direitos e privilégios e, portanto, abrangendo o direito a uma personalidade inviolável, justifica sozinho aquela ampla base sobre a qual pode repousar a proteção que o indivíduo exige". A privacidade é um pré-requisito para todos os outros direitos: liberdade de expressão, sexualidade, liberdade de consciência e segurança financeira dependem disso, porque nenhum direito pode ser exercido na presença de storm troopers batendo à porta. E por isso o direito de trancar essa porta é essencial.

Curiosamente, o artigo de Brandeis-Warren foi uma resposta a desenvolvimentos tecnológicos que ameaçavam a privacidade pessoal. Um dos desenvolvimentos foi a câmera portátil, com a qual jornalistas fotografavam pessoas importantes em locais que antes eram privados, como restaurantes, casamentos e funerais. Hoje, o foco da proteção da privacidade mudou dos jornalistas para o estado, para o qual "privacidade" é sinônimo de "sigilo". A privacidade não é mais um direito, mas uma provável causa de suspeita. A mudança na definição reflete o quão poderoso o estado se tornou desde a década de 1890 – e o quão enfraquecido se tornou o indivíduo.

Embora a privacidade tenha sido um tema tanto no direito consuetudinário quanto nas sociedades ocidentais, seu status legal tem sido vago. De fato, antes do "Direito à Privacidade", a proteção legal da privacidade era fragmentada em questões específicas. Leis contra invasão existiam, por exemplo, mas a codificação do conceito amplo de privacidade não existia.

Afinal, o que significa o "direito de ser deixado em paz"? Grande parte deste capítulo explora uma resposta.

Todo mundo sabe que a bolsa de uma mulher não deve ser roubada, nem sua janela espiada e tão pouco sua casa assaltada. Esses são obviamente e intuitivamente casos de violações de privacidade, mas não são o tipo de violação que os usuários de criptomoedas provavelmente enfrentarão. Os usuários de criptos lidarão com suas informações pessoais sendo extraídas e monitoradas – muitas vezes secretamente – para serem usadas contra eles de alguma maneira. Com o estado, o objetivo da extração de dados e do monitoramento é o controle social, a tributação, o confisco e a prisão. Com criminosos, o objetivo é o roubo, a chantagem e a extorsão.

Espiar pela janela do quarto pode ser uma violação óbvia de privacidade, mas e os bisbilhoteiros que acessam informações públicas, como as incorporadas à blockchain? O registro financeiro aberto da blockchain permite que partes indesejadas monitorem transações financeiras que os usuários tornam públicas voluntariamente. Se um bisbilhoteiro analisa o padrão de transferências e desmascara a identidade de um usuário, então a privacidade foi violada? A blockchain é uma rede pública, onde as pessoas trocam voluntariamente de uma maneira que sabem ser transparente e registrada. Espionagem é semelhante a ouvir pessoas que estão falando audivelmente em público. Mas será que ouvir é um ato culposo, especialmente quando feito por agentes do estado ou outros maus agentes? De fato, o estado e outros criminosos usam a informação de maneira maléfica, mas essa questão é irrelevante para definir se o ato de simplesmente ouvir é errado em si.

Avaliar essa questão significa colocar a privacidade no contexto de outros direitos humanos.

O contexto dos direitos humanos à privacidade

Murray Rothbard afirma que todos os direitos humanos são direitos de propriedade. Ou seja, todos os direitos se resumem à questão de quem controla adequadamente o uso e o descarte de uma coisa, seja a coisa uma ferramenta, uma ideia ou um corpo humano. É sempre possível usar a força para usurpar o controle de qualquer coisa, é claro, mas a questão de quem é o proprietário *adequado* permanece.

Rothbard responde: O proprietário é o indivíduo que detém o título válido da coisa. A verdadeira propriedade não é uma questão de *puro* controle, que pode ser adquirido através da força bruta, mas de controle legítimo, que vem da aquisição pacífica do título. Não pode haver título mais óbvio ou válido do que aquele que os indivíduos têm sobre seus próprios corpos. De fato, tentar negar esse título se reduz à obscenidade ou ao absurdo. Existem apenas três posições possíveis sobre quem possui o corpo de uma pessoa: a própria pessoa (liberdade), outra pessoa (escravidão), ou é bagagem não reclamada. Aqueles que valorizam a liberdade e os direitos humanos defendem a autopropriedade.

Novamente, a definição clássica de autopropriedade: todo ser humano tem jurisdição moral e lógica sobre seu próprio corpo e o uso

pacífico dele, incluindo os produtos de seu trabalho. Nenhum direito é mais fundamental do que a autopropriedade, porque ela é a própria fonte de todos os outros direitos. A liberdade de consciência e de expressão só existe porque os indivíduos têm a capacidade de pensar e falar, e ambos são aspectos do corpo humano. O direito de autodefesa existe apenas porque as pessoas são donas de seus corpos e têm o direito de proteger sua propriedade. O outro lado dos direitos é o dever. Assim como todos os outros seres humanos são moral e logicamente proibidos de iniciar a força contra você, você tem o dever de desistir de iniciar a força contra eles.

Se existe um direito à privacidade, então ele deve estar enraizado na autopropriedade. Deve ser o que se chama de direito natural. E, se a privacidade é um direito, outras pessoas têm o dever de desistir de violá-la.

A questão não é trivial. A propriedade de si mesmo e a privacidade estão ambas sob o constante ataque do maior bisbilhoteiro da história: o estado. O estado, com extremo preconceito, pretende usar os dados que coleta contra as pessoas. Em seu livro, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, o cientista político James C. Scott comenta o papel que apenas uma forma de coleta de dados desempenhou na ascensão do estado moderno: o censo. “Se imaginarmos um estado que não tem meios confiáveis de enumerar e localizar sua população, medir sua riqueza e mapear suas terras, recursos e assentamentos, estamos imaginando um estado cujas intervenções nessa sociedade são necessariamente brutas.” O estado atual é sofisticado e complexo.

Informação é poder, tanto para o indivíduo quanto para o estado. Uma razão pela qual o estado consegue adquirir dados é que a privacidade é um conceito mal definido que as pessoas não entendem como parte do contexto mais amplo dos direitos. Outra razão é que a informação é efêmera e parece menos propensa à posse do que uma mesa ou um carro.

A avaliação de se a privacidade de dados é um direito natural depende de duas questões. Como um prelúdio para considerá-las, pondere se você tem o direito de propriedade sobre seus pensamentos e sua expressão, incluindo a expressão de informações pessoais. Essa ampla indagação é fundamental para a questão da propriedade intelectual, que é a afirmação de que as ideias e suas expressões podem ser possuídas. As

pessoas chegam a conclusões dramaticamente diferentes, e a propriedade intelectual é frequentemente reivindicada como um direito natural. A mesma questão confronta a privacidade, que também aborda a propriedade das informações pessoais e a expressão delas.

Pergunta # 1: *Quem é o dono do que está na sua mente?*

A maioria das pessoas declararia em voz alta: "ninguém é dono do que está em minha mente!". Seus pensamentos são seus pela mesma razão que seus dedos e olhos; eles são parte de seu corpo, e seu corpo é quem você é. É você. Ninguém mais tem o que clamar ao reivindicar jurisdição sobre seu corpo. Mas e se o pensamento em sua mente for uma fórmula química originada por um colega de trabalho e escrita em um quadro-negro durante uma palestra que você assistiu? A fórmula agora faz parte da sua mente, assim como da dele e, se ele pode reivindicar o direito de usá-la porque faz parte do corpo dele, você não deveria poder fazer a mesma reivindicação?

Nesse ponto, o argumento do colega de trabalho geralmente muda de terreno. Ele *originou* a ideia, diz ele; a fórmula é um produto de seu trabalho, e possuir os produtos de seu trabalho é uma extensão da propriedade de si mesmo. Não importa se a ideia está em *sua* mente agora; é ideia *dele*. Ele a encontrou primeiro.

Deixando de lado o fato de que o colega de trabalho provavelmente utilizou as ideias e o trabalho de centenas de pessoas antes dele – ou seja, a fórmula também é produto do trabalho deles – vamos supor que ele adicionou um refinamento totalmente original. O que é que tem? No instante em que você vislumbrou a fórmula, o conceito mudou. A fórmula foi integrada a todos os outros conceitos que você tem sobre química, tecnologia e vida em geral. A fórmula em sua mente é ligeiramente ou consideravelmente diferente daquela no quadro-negro ou na mente de seu colega de trabalho. Como então ele pode reivindicar direitos de propriedade em uma ideia baseada no trabalho anterior de outras pessoas enquanto nega seus direitos de propriedade em uma ideia baseada em seu trabalho anterior?

A linha de chegada do cenário: ninguém tem direito ao que está em sua mente. O que é chamado de privacidade nesta circunstância se reduz à autopropriedade. Você é dono daquilo que está sob sua pele, incluindo as suas ideias. O libertário do século XIX James Walker afirma: "Meus pensamentos são minha propriedade, assim como o ar em meus pulmões é minha propriedade [...]" Quando você expira, no

entanto, você perde todo o direito de propriedade do ar expelido. O mesmo vale para ideias ou informações que são lançadas na esfera pública; você perde todas as reivindicações de privacidade, exceto e a menos que haja um acordo prévio de confidencialidade em vigor. Nessas circunstâncias, sua reivindicação de privacidade ou propriedade de informações não é uma questão de direitos naturais, mas de direitos contratuais.

O paralelo com as informações financeiras: os usuários de cripto perdem qualquer expectativa razoável de privacidade ou propriedade das informações quando elas entram na blockchain ou em outra esfera pública. Um bisbilhoteiro que acessa os dados nada mais faz do que ver aquilo que é de conhecimento e acesso público. O bisbilhoteiro pode usar o conhecimento de forma que prejudique um usuário, mas o uso da informação é uma questão diferente de como ela foi obtida.

Pergunta #2: *Como os dados foram obtidos?*

A resposta a esta pergunta é distinguir entre a espionagem legítima e o ato criminoso. Bisbilhoteiros legítimos não fazem mais que acessar informações divulgadas publicamente ou livremente e, ainda que sejam inconvenientes, de forma alguma violam direitos. Por outro lado, bisbilhoteiros criminosos violam direitos de propriedade privada para acessar dados. Tocar em um telefone ou computador é como invadir a casa de uma pessoa para vasculhar um arquivo ou uma mesa. Um recenseador que ameaça uma pessoa que não responde com multas ou prisão está usando meios criminosos para acessar informações. O teste decisivo para distinguir entre espionagem legítima e espionagem crime é se a aquisição de dados envolve uma violação de direitos.

Rothbard argumenta que “não existe direito à privacidade, exceto o direito de proteger a propriedade de uma invasão”. Em outras palavras, não há direito natural à privacidade per se. A informação é privada em virtude de estar protegida por outros direitos. Uma pessoa tem o direito de ocultar informações, por exemplo, porque o direito à liberdade de expressão inclui o direito de permanecer em silêncio, e quebrar um determinado silêncio requer ameaças ou violência. Da mesma forma, uma pessoa tem o direito de fechar a porta atrás de si, e as informações nos papéis em sua mesa são protegidas de intrusos por seu direito de propriedade sobre a casa. A privacidade da informação é protegida pelo muro de direitos que a cerca, mas isso não faz da privacidade um direito em si.

Por outro lado, se uma pessoa grita informações pessoais em praça pública ou se joga seus papéis pela janela ao vento, seus dados não estão mais protegidos por seus direitos de propriedade. A pessoa os colocou na esfera pública e abandonou a reivindicação de controle exclusivo.

A abordagem Satoshi da privacidade tem um pé em ambos os mundos – abandono público de informações junto com privacidade protegida por direitos naturais. Uma blockchain transparente funciona com usuários anônimos ou pseudônimos que empregam chaves públicas e privadas. Os dados sobre as transações foram jogados ao vento, mas as identidades são protegidas por outros direitos. Em outras palavras, desmascarar a identidade de alguém ou sua chave privada requer uma violação dos direitos de propriedade que os cercam e protegem – o direito da pessoa ao seu computador, por exemplo. A propriedade consiste no direito exclusivo de controlar e usar uma coisa; se o estado acessar um computador sem considerar o consentimento do proprietário real, então o estado está usurpando a propriedade do computador e violando descaradamente os direitos do proprietário real.

Uma mudança dramática no paradigma da privacidade

A abordagem Satoshi pode confundir algumas pessoas. Enquanto elas se apegarem ao velho paradigma de privacidade – isto é, privacidade é igual a ocultação – a transparência da blockchain continuará a soar como uma sentença de morte. Mas o novo paradigma da privacidade é a transparência das informações e a proteção da identidade. O foco mudou de informações sobre atividades para informações sobre nomes verdadeiros.

A transparência das transações serve a um propósito vital. Por uma questão de honestidade e eficiência, a blockchain publica todas as suas atividades. A proteção dos Nomes Verdadeiros também serve a um propósito vital. Por uma questão de liberdade pessoal, os participantes mascaram suas identidades à vontade e com facilidade. A blockchain exige a verificação de identidade tanto quanto uma mercearia exige o registro dos nomes daqueles que compram leite nela. Que todos vejam, que todos verifiquem a veracidade da transação. Que ninguém exija informações pessoais sobre quem é o porquê da troca. Tanto a honestidade

quanto a privacidade são preservadas, mas o vínculo entre uma transação e um Nome Verdadeiro é quebrado. O restabelecimento forçado desse vínculo ameaça a riqueza e a liberdade dos usuários.

No passado, o foco do estado era a divulgação ou vigilância forçada de informações sobre atividades, porque o estado havia encurralado a "indústria da identidade". Desde o nascimento, as pessoas são registradas, certificadas, gravadas e processadas de acordo com os números e outros identificadores emitidos pelo estado. David Friedman observa em seu ensaio "The Case for Privacy", "É difícil passar pelo mundo sem deixar rastros. Em algum lugar há um registro de todos os carros que comprei, todos os formulários de impostos que paguei, dois casamentos, um divórcio, o nascimento de três filhos, milhares de postagens em fóruns on-line sobre uma ampla variedade de assuntos, quatro livros publicados, registros médicos e muito mais."

A identidade e o Nome Verdadeiro dos indivíduos são muito mais conhecidos do que suas interações, muitas das quais podem ocorrer em segredo e silêncio. O modelo Satoshi inverte essa situação. Ele torna todas as interações públicas com todas as identidades permanecendo privadas a critério dos indivíduos. O estado não controla mais a identidade e, sem esse controle, o acesso a todas as outras informações têm pouco valor. E o estado sabe muito bem disso.

A era digital mudou o Zeitgeist cultural, político e psicológico da privacidade. "Cuide da sua maldita vida!" já foi uma atitude respeitada, mas o estado lentamente corrompeu a ideia de que pessoas inocentes precisam de privacidade. Eis o novo Zeitgeist: apenas aqueles que têm algo a esconder se recusam a responder a perguntas ou a serem observados. "Só os criminosos temem a vigilância do estado" é uma resposta comum para quem defende a privacidade hoje. Mas toda pessoa pacífica é agora um criminoso com algo a esconder. Por quê? Porque todos ultrapassaram o limite de velocidade, usaram drogas ilegais, contrabandearam bebidas baratas ou cigarros através da fronteira, fizeram acréscimos "não autorizados" a um imóvel, enganaram um agente do estado, sonegaram sua renda ou violaram uma das dezenas de milhares de leis estatais que criminalizam o comportamento inofensivo de maneira onipresente. A maioria das pessoas não está ciente de quantas leis eles quebram no decorrer de uma vida cotidiana pacífica.

Quando a Privacidade é Criminalizada, Apenas os Criminosos têm Privacidade

Em seu livro *Three Felonies A Day: How the Feds Target the Innocent*, o advogado Harvey Silverglate detalha como o americano médio acorda e segue sua rotina diária, sem saber que provavelmente cometerá vários crimes federais ao fazê-lo. O número de crimes federais aumentou exponencialmente nas últimas décadas e os promotores agora podem escolher entre uma infinidade de crimes vagamente definidos para acusar indivíduos pacíficos de todas as origens, profissões e status. Uma combinação de leis amplas e mal definidas, a guerra às drogas e promotores de carreira que são imunes às consequências transformaram a justiça em uma burocracia livre de consciência, onde parece não haver espaço para a inocência ou culpa. Silverglate observa um procedimento padrão para os burocratas da justiça:

> Os promotores são capazes de estruturar acordos de delação premiada, de maneira que torna quase impossível para pessoas normais, racionais e calculistas se arriscarem a ir a julgamento. A pressão sobre réus inocentes para se declararem culpados e "cooperar" testemunhando contra outros em troca de uma sentença reduzida é enorme – tão grande que essas testemunhas que cooperam muitas vezes deixam de dizer a verdade, dizendo, em vez disso, o que os promotores querem ouvir.

O livro de Silverglate evoca uma assustadora citação infame da era soviética, dita pelo desprezado Beria, chefe da polícia secreta de Stalin. "Mostre-me o homem, e eu encontrarei o crime para você." Quando alguém lhe perguntar: "O que você tem a esconder?", você deve responder: "De Beria e sua laia, tudo, especialmente minha identidade (o homem)."

Ou, como Ayn Rand explicou certa vez: "O único poder que qualquer estado tem é o poder de reprimir os criminosos. Bem, quando não há criminosos suficientes, eles os criam. Declara-se que tantas coisas são crime que se torna impossível para os homens viverem sem infringir as leis."

Os usuários de cripto que exigem privacidade são especialmente vulneráveis a suposições culturais e políticas que favorecem fortemente o controle estatal em vez da liberdade individual.

As fortes suposições contra a privacidade incluem:

- A presunção da inocência pertence ao estado, e não aos indivíduos.
- Um duplo padrão de moralidade é aplicado ao estado e aos indivíduos.
- A privacidade é equiparada à ocultação.

A Presunção da Inocência. O termo legal "presunção da inocência" às vezes é expresso pela frase latina "*ei incumbit probatio qui dicit, non qui negat*", que significa que o ônus da prova é do acusador, e não do acusado. O acusado é presumido inocente até que se prove o contrário. A doutrina jurídica baseia-se na crença de que a maioria das pessoas não são criminosas, de modo que a criminalidade não pode ser presumida; ela deve ser demonstrada. A doutrina também reconhece um princípio fundamental da lógica: por ser impossível provar uma negativa, o ônus da prova recai sobre a pessoa que faz uma afirmação positiva. Alguém pode alegar que você é um ladrão. E mesmo evidências massivas de sua honestidade não dissiparão a acusação, porque você pode estar mentindo sobre um delito passado ou ocultando evidências. É por isso que o acusador é solicitado a especificar o que você roubou e a fornecer provas do crime.

A presunção da inocência é a pedra angular do devido processo legal e um muro de proteção contra processos arbitrários por parte do estado. É uma característica definidora de uma sociedade livre em oposição a uma totalitária. O renomado advogado britânico Sir John Clifford Mortimer – mais conhecido como o criador do amado advogado de defesa fictício Horace Rumpole – estava longe de ser o único a ver a presunção da inocência como "o fio de ouro" que une a justiça.

Mas o fio de ouro foi rompido.

Em nome da segurança, o público perdeu a presunção da inocência mesmo na ausência de acusações. Agentes de fronteira e aeroporto tiram impressões digitais, revistam, interrogam e ladram "Seus documentos!" para hordas enfileiradas. Indivíduos que não cumprem são automaticamente retirados da linha e processados como criminosos. Os policiais exigem identidade e prendem aqueles que se recusam, independentemente de a prisão ser legal ou não. Afinal, supõe-se que os agentes estatais protejam a segurança e imponham a paz. Isso significa que aqueles que resistem são contra a segurança e a paz. Poucas pessoas

perguntam de onde a imposição da lei obtém o direito de exigir obediência de pessoas que não estão causando danos. A presunção de inocência foi transferida dos indivíduos para os agentes estatais, o que inverte a intenção original do conceito legal de proteger os indivíduos *do* estado.

O princípio lógico de ser incapaz de provar uma negativa foi substituído pela falácia conhecida como "o argumento ou apelo à ignorância". Aqui, "ignorância" refere-se à falta de evidência contrária – uma situação considerada suficiente para provar a verdade de uma afirmação. Em suma, uma acusação é verdadeira porque não se prova que seja falsa. A criminalidade de um indivíduo torna-se um dado porque não é refutada. Por que mais, pergunta o estado, ele se recusaria a cooperar com as autoridades?

É difícil exagerar a importância da mudança na presunção da inocência do indivíduo para os agentes estatais. Assim como a presunção da inocência é o fio de ouro da justiça, a presunção da culpa para os indivíduos é sua morte. Isso oblitera o devido processo e leva a sociedade diretamente para o totalitarismo. Esse é o significado político e a consequência da "inocente" pergunta: "O que você tem a esconder?". A identidade emitida pelo estado é crucial para o processo. Depois que seu Nome Verdadeiro é conhecido, então todos os outros controles sociais se tornam possíveis.

Um duplo padrão de moralidade. Existem dois pesos e duas medidas em ação na sociedade – um para os indivíduos e outro para o estado. O que é imoral para um indivíduo, tornou-se moral para o estado. Se você pegar dinheiro de um vizinho sob a mira de uma arma, é um ato de roubo pelo qual você é preso com justiça. Se um agente do estado faz o mesmo, é um ato de tributação, pelo qual o malfeitor paga sua "justa parte" dos ganhos e pelo qual o agente recebe um salário e uma pensão. A moralidade moderna é agora definida por quem está realizando o ato, não pelo ato em si. O sigilo impenetrável do estado é prudente, enquanto a privacidade dos indivíduos é criminosa.

Nenhuma voz foi mais clara contra um duplo padrão de moralidade do que a do editor libertário Raymond Cyrus Hoiles, que criou a rede midiática Freedom Communications. Hoiles acreditava que o duplo padrão era mais destrutivo para a sociedade do que qualquer outro conceito, e seus ataques ferozes contra ele explodiam com frequência em seus jornais.

Em um editorial intitulado "O erro mais prejudicial que a maioria das pessoas honestas cometem" (17 de dezembro de 1956), publicado no *Santa Ana Register*, Hoiles explica o erro: "É a crença de que um grupo ou um estado seja capaz de fazer coisas que seriam prejudiciais e perversas se feitas por um indivíduo e produzir resultados que não sejam prejudiciais, injustos e perversos. É a crença de que um número de pessoas fazendo algo que é errado para um indivíduo pode resultar em algo correto e justo." Hoiles mais frequentemente criticou o erro com referência à tributação. Novamente, se era errado um vizinho roubar seus bens, então era igualmente errado para um grupo de vizinhos ou seu representante designado (estado) realizar o mesmo ato.

A crítica de um duplo padrão não começou com Hoiles, é claro. Um panfleto de 1657 atribuído ao rebelde Coronel Titan argumenta: "O que pode ser mais absurdo na natureza e contrário a todo bom senso do que matar e chamar de Ladrão aquele que vem sozinho […] e obedecer e chamar de Lorde Protetor aquele que vem com regimentos e tropas? Se aquele que rouba e comanda dois ou três navios é chamado de pirata, por que aquele que rouba e comanda cinquenta é chamado de almirante?". É esse o absurdo que o estado impõe quando faz algo que não seria tolerado caso fosse feito por um único indivíduo.

Mais uma vez, ninguém pergunta onde o estado adquire esses chamados direitos abrangentes. Como os únicos direitos que existem são os individuais, contra os quais ninguém pode legitimamente agredir, se o estado deseja reivindicar a propriedade legítima das informações privadas de terceiros deve apresentar prova de divulgação voluntária, transferência ou compartilhamento de título. Caso contrário, os chamados direitos nada mais são do que a afirmação da pura violência.

O que se aplica à tributação se aplica não menos à violação da privacidade. Se é errado um vizinho revistar seu corpo e o de seu filho sem consentimento, então é errado um agente do estado fazer isso em um aeroporto. Se é errado um vizinho grampear seu telefone, registrar suas transações financeiras e espiar pelas janelas, então é errado o estado fazê-lo. Os indivíduos de um grupo não renunciam à responsabilidade pessoal porque os atos são sempre cometidos por um indivíduo e são sempre uma questão de responsabilidade pessoal. O estupro coletivo não é menos que o estupro individual e os estupradores não são menos particularmente responsáveis porque foram o segundo ou o terceiro na fila.

No entanto, as pessoas aceitam um duplo padrão de moralidade, que isenta os agentes estatais de responsabilidades morais e legais. Se os agentes do estado, do presidente aos funcionários dos correios, estivessem sujeitos aos mesmos padrões de decência e responsabilidade legal que os indivíduos, o atual estado desmoronaria.

A privacidade é equiparada à ocultação. Redefinir "privacidade" como "ter algo vergonhoso a esconder" é um truque de mágica. Em seu excelente ensaio "I've Got Nothing to Hide' and Other Misunderstandings of Privacy", o professor Daniel J. Solove explica a mágica por trás da metamorfose da privacidade em ocultação: "O argumento de que não existe problema de privacidade se uma pessoa não tem nada a esconder é frequentemente feito. […] Quando o governo se envolve em vigilância, muitas pessoas acreditam que não há ameaça à privacidade, a menos que o governo descubra atividades ilegais, caso em que uma pessoa não tem justificativa legítima para alegar que isso deve permanecer privado". Curiosamente, as pessoas que usam o argumento de não ter "nada a esconder" também penduram cortinas nas janelas e as fecham ao se despir. Eles não dão suas carteiras ou bolsas para estranhos vasculharem. Eles fecham a porta antes de fazer sexo e se opõem que suas fotos nuas sejam postadas online. O que eles estão escondendo? Como Solove comenta: a privacidade "não é sobre nada a esconder, é sobre as coisas que não são da conta de ninguém."

O ataque à privacidade individual é tóxico para a sociedade como um todo.

Considere a liberdade de expressão. Lembro-me de estar em um restaurante quando um parente fez um discurso pós 11 de setembro sobre como a atmosfera nos EUA estava começando a parecer a da Cuba da qual ele havia fugido. Sua esposa tentou silenciá-lo, declarando em um sussurro inflexível: "Você não pode dizer essas coisas em público". Ela estava nervosa enquanto olhava ao redor para ver quem poderia ter ouvido. A vigilância e os informantes tornam as pessoas relutantes em expressar opiniões que podem ser usadas contra elas de maneira legal ou política. Propriedades podem ser apreendidas, famílias destruídas e pessoas presas. Por que alguém falaria o que pensa se como resultado seus filhos podem perder o pai deles?

Até recentemente, muitas incursões contra a privacidade não ocorriam apenas por serem difíceis de executar. Então a tecnologia chegou. A vigilância agora é muito mais eficiente, e requer menos esforço.

Mesmo burocracias notoriamente incompetentes são capazes de vigiar como nunca. Muitas pessoas estão com medo ou complacentes em relação à vigilância. Alguns simplesmente não acreditam mais na possibilidade de privacidade. O estado se beneficia imensamente da Grande Mentira de que a privacidade agora é impossível devido à onipotência e onisciência do estado. Isso é besteira. Em primeiro lugar, a tecnologia quase sempre empodera o indivíduo tanto ou mais do que o estado. Em segundo lugar, há um mundo de diferença entre o mais difícil e o impossível. A privacidade pode ser mais difícil do que antes ou, talvez, seus requisitos tenham apenas mudado e sejam necessárias proteções diferentes do que as de antes. Talvez a privacidade exija mais inovação e trabalho.

O valor da privacidade para a sociedade

Uma sociedade saudável requer privacidade. Quando um estado monitora a comunicação geral, as pessoas não interagem livremente. Isto é especialmente verdadeiro para dissidentes, os pacificamente aberrantes, escritores, delatores, usuários de drogas, críticos do estado, céticos, advogados de defesa, artistas … Quem é diferente no estilo de vida ou na opinião sente o calafrio de ser observado por autoridades que acenam com armas e celas de prisão. A sombria sociedade cinzenta da União Soviética e de outros estados comunistas fornecem uma lição de moral sobre como o medo esmaga a criatividade e a discussão. A vigilância despoja a sociedade de cor e vibração porque drena a vida dos indivíduos, e os indivíduos *são*, coletivamente, a sociedade.

Também impede que as pessoas se levantem contra a injustiça. A defesa da privacidade é uma defesa dos direitos humanos. Ainda assim, a privacidade financeira pode não ser a questão com a qual entrar na discussão desse vínculo, porque o dinheiro desperta cinismo imediato. Mas o vínculo deve ser estabelecido.

Considere a liberdade de religião e o devido processo legal. Uma insurreição do século XVI definiu a evolução desses dois, bem como sua conexão com a privacidade. A revolta girava em torno do direito de uma pessoa manter suas crenças religiosas privadas para que não pudessem ser usadas contra ela em um tribunal. Uma versão atual desse direito é chamada de “clamar a quinta” – invocando o devido processo

legal contra a autoincriminação. É chamado de "clamar a quinta" porque a Quinta Emenda da Declaração de Direitos dos EUA estabelece: "Nenhuma pessoa será obrigada em qualquer caso criminal a ser testemunha contra si mesma". Embora este pilar do devido processo seja frequentemente retratado como um recurso para o culpado, o grande beneficiário é o homem inocente na rua, que é protegido contra o exercício do poder arbitrário, quer ele perceba ou não.

A insurreição do século XVI: Henrique VIII negou a autoridade papal e estabeleceu a Igreja da Inglaterra, que reivindicou nova autoridade sobre as almas das pessoas. Os protestantes, chamados dissidentes, eram frequentemente julgados por heresia com tortura, geralmente acompanhando o julgamento. No final da década de 1530, o protestante John Lambert foi queimado vivo por heresia. Durante seu julgamento, Lambert se tornou o primeiro inglês conhecido a proclamar que era ilegal sob Deus e a lei comum obrigar um homem a se acusar. Ele apelou para a privacidade da consciência.

Em 1563, o dissidente John Foxe publicou o imensamente influente *Book of Martyrs*, um livro de história e martirológio protestante, que foi chamado de "cartilha libertária" sobre direitos processuais. Ele defende o direito de permanecer em silêncio para manter as informações pessoais privadas. Notoriamente, o leveller e libertário John Lilburne empregou os procedimentos de Foxe em 1637, quando foi levado ao Tribunal da "Star Chamber" (Câmara Estrela) por distribuir livros puritanos (o termo "Star Chamber" tornou-se sinônimo de tribunais elitistas e abusivos que se reúnem em segredo). Recusando-se a fazer o juramento costumeiro, Lilburne negou-se a responder perguntas que testemunhassem contra si mesmo. Ele foi multado, chicoteado, humilhado e condenado à prisão até que ele obedecesse. Enquanto estava lá, ele escreveu um relato de seu tratamento brutal, intitulado *The Work of the Beast*. Alguns anos depois, a tão odiada Star Chamber foi abolida e o direito de permanecer em silêncio – o direito à privacidade – foi estabelecido.

O direito contra a autoincriminação – o direito à privacidade das informações pessoais – está no cerne do devido processo legal. Está historicamente ancorado na busca pela liberdade religiosa, mas não se aplica menos a outras liberdades, inclusive às econômicas. A demanda por privacidade não apenas protegeu os indivíduos, mas também impulsionou as sociedades em direção à liberdade.

É apenas um pequeno exagero dizer que a Revolução Americana poderia não ter ocorrido se os colonos não tivessem exigido o direito à privacidade pessoal e de propriedade. A privacidade é um princípio e uma virtude revolucionária que levou os colonos americanos a fechar a porta na cara das autoridades britânicas, literal e figurativamente. A Terceira Emenda da Constituição dos EUA, por exemplo, proíbe a prática então generalizada de alistar soldados à força em residências particulares, mesmo em tempos de paz. A Emenda soa antiquada aos ouvidos modernos, mas a violação foi importante o suficiente para que os revolucionários a colocassem em terceiro lugar na lista de liberdades declaradas pela Declaração de Direitos. A Terceira Emenda afirma o direito à privacidade contra a intrusão do estado no mais pessoal de todos os reinos: o lar. Por mais ultrapassada que essa emenda possa parecer, não é necessário um grande salto para aplicar seu princípio ao atual ataque contra todas as outras formas de privacidade.

A Quarta Emenda também afirma a privacidade. Começa defendendo "[o] direito do povo à segurança de suas pessoas, casas, papéis e pertences contra buscas e apreensões irrazoáveis". Em termos de privacidade, a palavra importante é "papéis", porque pode ser extrapolada para se aplicar a e-mails e outros dados de computador, incluindo identidades reais.

A Quinta Emenda defende a privacidade ao decretar o direito de um indivíduo *de não* prestar "testemunha contra si mesmo" em casos criminais.

No linguajar do século XVIII, quando o estado vigia computadores e contas de cripto, ele está realizando uma apreensão de "papéis". No entanto, as regras de provas físicas nem sempre se aplicam de forma clara às provas digitais, e as decisões inconsistentes dos tribunais sobre privacidade das criptos causam confusão. A compreensão da crescente confusão legal sobre privacidade pode estar na palavra da Quarta Emenda – "papéis". A Emenda afirma que tanto "papéis quanto pertences [estão protegidos] contra buscas e apreensões irrazoáveis". Mas o direito consuetudinário, no qual se baseia a jurisprudência ocidental, tende a conceder maior proteção aos "papéis" do que aos "pertences", talvez porque os documentos sejam vistos como uma violação da pessoa e não da propriedade.

O professor de direito Donald A. Dripps abre seu ensaio pioneiro "'Dearest Property': Digital Evidence and the History of Private 'Papers' as Special Objects of Search and Apprehension" com duas perguntas. "Por que a Quarta Emenda se refere distintamente a 'papéis' antes de 'pertences'? Por que devemos nos importar?" Dripps pede para "fundar regras especiais da Quarta Emenda para evidências digitais" dentro da lei estatal para restringir "o volume de informações inocentes e íntimas que devem ser expostas [ou exigidas] antes que o material criminal seja descoberto". Mais uma vez, a Revolução Americana fornece uma visão.

Na década de 1760, os mandados britânicos para documentos começaram a ser emitidos contra autores e editores coloniais suspeitos de sedição. *Entick V. Carrington* (1765) é provavelmente o caso jurídico mais influente da época. Os fatos básicos do caso: John Entick publicou um jornal que se opunha à Coroa. Em 1762, oficiais invadiram a casa de Entick e roubaram centenas de papéis em busca de evidências de traição. Entick processou. Entick ganhou. O juiz presidente, Lorde Camden, ofereceu um famoso ditado: "Se for lei, será encontrado em nossos livros. Se não for encontrado aqui, não é lei". O suposto direito do estado de apreender papéis não estava nos estatutos, portanto, não era lei.

A análise subsequente do caso *Entick* descobriu que quatro aspectos do ataque do estado eram legalmente desagradáveis; todos eles se aplicam à atual vigilância e apreensão de informações financeiras. O mandado foi *indiscriminado*. A apreensão expropriou os papéis, negando seu uso ao autor. O mandado foi desregulado porque não havia supervisão neutra ou via de apelação. A apreensão foi *inquisitorial* porque deu ao estado informações sobre o funcionamento privado da mente de Entick. O advogado de Entick declarou: "Nenhuma potestade pode invadir legalmente a casa de um homem e investigá-la para buscar provas contra ele; isso seria pior do que a inquisição espanhola, pois saquear as gavetas e caixas secretas de um homem para obter provas contra ele é como torturar seu corpo para descobrir seus pensamentos secretos." A apreensão de papéis era um ataque contra a pessoa, não contra a propriedade.

Qualquer juiz que posteriormente considerasse emitir um mandado de busca de documentos tinha que considerar a decisão de Lorde

Camden: de que uma suposta ofensa precisava estar nos livros de estatuto para que existisse na lei. Além disso, mandados sobre documentos cada vez mais entravam em conflito com as constituições estaduais.

A guerra muda as leis, especialmente as leis que protegem os direitos individuais. Dripps continua: "A América se recusou a modificar a proibição da lei comum por estatuto até a Guerra Civil". O imposto de consumo era a principal fonte de financiamento do governo federal para a guerra, mas a evasão fiscal era desenfreada. Em resposta, um estatuto único foi aprovado. "[Este] ato de 1863 foi o primeiro ato neste país [...] ou na Inglaterra, até onde pudemos apurar, que autorizou a busca e apreensão de documentos particulares de um homem, ou a produção compulsória deles, para usá-los como prova contra ele em um processo criminal, ou em um processo para executar o confisco de seus bens". A apreensão de papéis estava agora nos estatutos.

A questão dos papéis versus pertences ziguezagueou juridicamente após a Guerra Civil. Indiscutivelmente, a mudança mais importante ocorreu em 1886, quando o *Boyd v. United States* foi decidido pela Suprema Corte dos EUA. "A história do caso Boyd", escreve Dripps, "começa corretamente com um estatuto que autoriza os funcionários da alfândega a apreender os livros e papéis de importadores suspeitos de evasão de impostos". A Suprema Corte decidiu a favor de Boyd, dizendo:

> "Os princípios estabelecidos neste parecer afetam a própria essência da liberdade e da segurança constitucionais. Aplicam-se a todas as invasões por parte do estado e seus funcionários à santidade da casa de um homem e das privacidades da vida. Não é o arrombamento de suas portas e o remexer de suas gavetas que constitui a essência da ofensa, mas sim a invasão de seu direito irrevogável de segurança pessoal, liberdade pessoal e propriedade. É a invasão desse direito sagrado que fundamenta e constitui a essência do julgamento de Lord Camden."

A decisão de *Boyd* restabeleceu maior proteção constitucional aos papéis do que aos pertences, e incide diretamente sobre os papéis digitais. A proteção nunca foi absoluta, no entanto, e foi severamente cor-

rompida. Dripps explica: “Durante o último quarto do século XX, a Suprema Corte começou efetivamente a equiparar ‘papéis’ e ‘pertences’. Outra linha de casos modernos estabeleceu regras de ‘linhas-claras’, que deram o mesmo tratamento constitucional a todos os ‘pertences’”. Os papéis não apenas perderam seu status especial sob o direito comum e constitucional, mas também chegaram mais perto de se tornarem legalmente intercambiáveis com todos os outros pertences. Isso oferecia uma proteção muito mais fraca. No entanto, o precedente de *Boyd* prevaleceu por quase um século e ainda não envelheceu.

A importância dos papéis está intrinsecamente ligada ao valor da privacidade para os indivíduos. Quando o estado rouba dados, não viola “propriedades” no sentido legal da palavra; ele viola a pessoa.

A privacidade faz parte de uma vida saudável, criativa e autorreflexiva. Desde a infância mantenho um diário no qual coloco esperanças, confusões, decepções e desejos. Quando leio páginas do passado, me conecto visceralmente com quem eu era aos dez anos e entendo melhor a pessoa que sou hoje. Esses diários são privados, não porque eu tenha vergonha deles, mas porque são *pessoais*. Em seu romance distópico 1984, George Orwell enfatiza a importância dos diários:

> “A única coisa que ele estava prestes a fazer era abrir um diário. Isso não era ilegal (nada era ilegal, já que não havia mais leis), mas se detectado era razoavelmente certo que seria punido com a morte.”

O protagonista de *1984* descobre seu individualismo. Nesta jornada, o diário representa a liberdade de expressão e consciência que são essenciais para um senso de identidade – tão essencial que o estado matará por esse ato de privacidade.

Toda violação de privacidade corrói o espírito humano. Uma palavra não é dita por medo de ser ouvida; um pensamento não se forma por medo de se tornar uma palavra; um sentimento nunca é expresso e, talvez com o tempo, nem mesmo sentido. Então, um dia, o silêncio exterior torna-se interior através do hábito agora automático da autocensura. As pessoas não questionam mais. Talvez nem percebam mais que não questionam mais. Eles desenvolveram o hábito de não ser um indivíduo e, em vez disso, tornaram-se parte de uma vontade coletiva.

Todo mundo tem áreas de privacidade para proteger. Alguns usam medalhões com fotos de parentes mortos; outros abrigam um amor proibido; alguns trancam a porta para deleitar-se com um banho quente sem serem incomodados, ou escondem uma preferência sexual incomum. Todo ser humano tem o direito de traçar linhas que não prejudicam ninguém, linhas que ninguém mais deveria cruzar sem ser convidado. Bata a porta na cara de quem disser o contrário!

O foco das criptomoedas na privacidade é mais do que o desejo de reter riqueza, como geralmente é acusado. É um desejo de manter a individualidade, o espírito humano e a liberdade.

Nomes Verdadeiros e Estratégias para a Privacidade

> Todos aqueles que usaram seu conhecimento em uma tentativa de promover mudanças sociais viram a criptografia como uma ferramenta para aumentar a privacidade individual e transferir o poder das grandes instituições centrais para os seres humanos que vivem em sua órbita.
> – Paul Vigna.

O mundo precisa de um novo paradigma de privacidade porque o Estado sempre vencerá sob o velho paradigma enquanto controlar a Indústria de Identidade. A indústria consiste em muito mais do que documentos de identificação do governo e formulários a serem preenchidos. Nas últimas duas décadas, a Indústria da Identidade se expandiu para incluir triagem de aeroportos, biometria, regulações Know Your Customer, caches de dados clandestinos e vigilância em cada turno. Alastair Berg, do RMIT Blockchain Innovation Hub, observa: “Esses são apenas alguns segmentos em uma indústria que deve crescer para $16 bilhões até 2022”.

O Estado não vai afrouxar o controle sobre a indústria porque a identificação é uma parte insubstituível do controle social e da acumulação de riqueza. Isso é verdade desde a era napoleônica, quando foi introduzido um cartão de identidade que prenunciava os modernos. O objetivo do ID era controlar os salários, restringindo a mobilidade dos trabalhadores que queriam se mudar para obter melhores empregos com salários mais altos. As cartas foram fundamentais para converter uma França relativamente livre em um estado policial.

O monopólio estatal de identificação precisa ser quebrado da mesma maneira que as criptos quebram o monopólio monetário. Não deve ser confrontado; ele deve ser contornado, procurando-se uma alternativa melhor. Isso não apenas afasta o Estado, mas também fornece uma alternativa de livre mercado para a necessidade humana válida de identificação. Historicamente, a identificação era uma função de livre mercado; certidões de casamento, por exemplo, eram um contrato privado entre famílias e honrados pela igreja. Pode facilmente ser uma função do livre mercado novamente. Enquanto a Indústria da Identidade

for um ramo do governo, no entanto, essa necessidade humana ficará insatisfeita ou será satisfeita a um custo assombroso para a liberdade.

O novo paradigma online para privacidade está aqui. É exemplificado pela blockchain onde as interações são transparentes e as identidades reais são protegidas. A privacidade reside na proteção de True Names (Nomes Verdadeiros) – uma referência à novela pioneira de 1981, de Vernor Vinge, na qual um grupo de hackers (chamados warlocks/feiticeiros) invade computadores ao redor do mundo. Suas identidades reais são secretas umas das outras e especialmente do Grande Adversário – uma referência ao estado americano. Mascarar identidades do mundo real é vital porque qualquer um que conheça o True Name de um "feiticeiro" pode chantageá-lo ou causar uma True Death (Morte Verdadeira). A identidade é literalmente uma questão de vida ou morte.

A origem dos True Names

> "Acho que o carteiro está nos atacando um de cada vez, começando com os mais fracos, nos atraindo o suficiente para aprender nossos Nomes Verdadeiros – e então nos destruindo."
> – Vernor Vinge, *True Names*

True Names é uma das primeiras representações ficcionais de um ciberespaço desenvolvido. É amplamente creditado como iniciador do movimento cyberpunk, que mais tarde explorou muitos dos temas apresentados na novela.

A novela começa da seguinte maneira:

> Nos dias de era-uma-vez da Primeira Era da Magia, o feiticeiro prudente considerava seu próprio nome verdadeiro como seu bem mais valioso, mas também a maior ameaça à sua vida, pois – as histórias contam – uma vez um inimigo, mesmo um inimigo fraco e não qualificado, aprendeu o verdadeiro nome do feiticeiro, e então feitiços rotineiros e amplamente conhecidos poderiam destruir ou escravizar até mesmo os mais poderosos. Com o passar dos tempos, chegando à Idade da Razão, e daí para a primeira e a segunda revoluções industriais, tais noções foram desacreditadas. Agora parece que a Roda deu uma volta completa (mesmo

> que nunca tenha havido realmente uma Primeira Era) e voltamos a nos preocupar com nomes verdadeiros novamente.

Na história, o hacker protagonista é visitado por agentes do Grande Inimigo que descobriram seu Verdadeiro Nome. Eles o armam para rastrear um alvo maior conhecido como The Mailman. Assim, a história é altamente antiestatista com um senso aguçado de como a identidade é crucial para a liberdade.

A novela despertou a admiração dos criptoanarquistas, que também se basearam em sua visão do ciberespaço. Uma reimpressão posterior de *True Names* inclui dez artigos e ensaios de escritores que fornecem comentários sobre a história de Vinge. Um deles é o ensaio "True Nyms and Crypto Anarchy" de Timothy May, autor de "The Crypto Anarchist Manifesto". (Nyms é a abreviação de pseudônimos.) No tributo a *True Names,* May afirma com otimismo:

> "A criptoanarquia é a realização ciberespacial do anarcocapitalismo, transcendendo as fronteiras nacionais e liberando os indivíduos para fazer consensualmente os arranjos econômicos que desejam fazer."
> Isso garante que homens com armas não possam ser trazidos para interferir em transações mutuamente acordadas, o único tipo de interação econômica possível na anarquia criptográfica. Algumas pessoas, é claro, gritarão: "Injusto!", e exigirão a intervenção do governo, razão pela qual a criptografia pesada provavelmente sofrerá oposição das massas, a menos, é claro, que as massas sejam sábias e tenham uma visão de longo prazo. Isso pode cheirar a elitismo, mas tenho muito pouca fé na democracia. De Tocqueville alertou em 1840 que, traduzido aproximadamente: "A República Americana durará até que os políticos percebam que podem subornar as pessoas com seu próprio dinheiro". Chegamos a esse ponto há várias décadas.

A criptografia pesada e a privacidade que ela oferece são essenciais para o sucesso da criptoanarquia. Sua antítese é o controle social, que requer identificar as pessoas e vinculá-las às atividades para ser eficaz. A criptografia quebra esse vínculo. E nunca é cedo demais.

Atualmente, a identidade do governo é a única maneira pela qual a maioria das pessoas pode provar suas identidades offline para acessar as necessidades da vida moderna. Na maioria dos países ocidentais, pessoas indocumentadas não podem embarcar em um avião, dirigir um carro ou alugar um apartamento. Elas não podem abrir uma conta bancária, adquirir um cartão de crédito, acessar cuidados médicos, descontar um cheque, ter um emprego visível, frequentar uma universidade ou comprar um carro. Tornam-se cidadãos de segunda classe.

Enquanto isso, aqueles com identidade estatal tornam-se vulneráveis a processos e perseguições. Em um sistema nacionalizado de identificação e relatórios, o governo sabe quem são todos, o que cada um possui e onde encontrar ambos. Como Orwell argumenta eloquentemente em romances e ensaios, a nacionalização da privacidade é um pilar do totalitarismo. Não é de admirar que o apetite do governo por dados seja tão voraz. Não é à toa que há um esforço para retirar o anonimato da Internet sob a égide da preocupação com o bullying.

O que é necessário agora é um novo paradigma para a privacidade offline que possa funcionar em conjunto com as proteções online. Ou melhor, um velho paradigma deve ser revivido. A privacidade offline é melhor alcançada pelo ID de livre mercado, que fornece os benefícios da identificação sem a responsabilidade de se tornar um número em um arquivo burocrático.

Sistemas offline de identificação de livre mercado

A identidade de livre mercado é a antítese da identidade do governo na medida em que devolve o poder de identificação ao indivíduo para usar ou não de acordo com seu próprio critério. A identidade de livre mercado é uma aliada natural da criptografia, porque os objetivos são os mesmos – quebrar o monopólio estatal da indústria de identidade.

Quando o comércio estava no nível do escambo, as pessoas geralmente conheciam os indivíduos com quem negociavam. Quando o comércio se expandiu para incluir trocas complexas com estranhos a um mundo de distância, a troca direta foi substituída pela troca indireta, que muitas vezes exigia confiança ou um intermediário. A base da confiança em alguém é a capacidade de responder à pergunta: “Com quem estou lidando?”. Assim, há uma necessidade legítima de identificação e pouco perigo para ela enquanto o estado não estiver envolvido.

Considere um método difundido de identificação de séculos atrás que está voltando – cartas de apresentação. A dinâmica básica: a pessoa A carrega cartas de identificação para a pessoa C a quem A é um estranho. As cartas são escritas pela pessoa B, que é um conhecido respeitado e mútuo. A pessoa B atesta a identidade do portador da carta e C é capaz de responder à pergunta: “Com quem estou lidando?”. Essas cartas podem ser preparadas por uma empresa que verifica identidades para obter lucro.

Uma versão eletrônica de cartas de apresentação ocorre em círculos de criptografia e em redes sempre que um membro respeitado atesta um estranho que deseja participar. Dado o tamanho da comunidade e o fato de estar sob ataque, as introduções parecem ser uma prática cada vez mais popular.

As cartas incorporam o primeiro e mais básico serviço prestado pelo ID do livre mercado: a *autenticação*. Existem inúmeras razões pelas quais alguém gostaria de autenticar a identidade de uma pessoa. A pessoa pode estar pegando um pacote, confirmando uma reserva, ingressando em um clube, descontando um cheque ou solicitando um emprego. O filtro de autenticação significa que um estranho não pode cometer fraudes.

A autenticação no livre mercado de identidades reais também pode ser realizada por empresas que emitem carteiras de identidade. A identificação privada é comum hoje em uma forma bastarda que tem valor limitado. Os empregadores emitem IDs aos funcionários para que possam desbloquear escritórios; as instituições financeiras oferecem cartões de crédito aos clientes; as universidades distribuem carteiras de identidade para que os alunos possam acessar os serviços. Mas a privacidade aqui é ilusória. Antes que um empregador ou uma instituição financeira emita o ID, o destinatário é selecionado no processo de contratação ou na abertura de uma conta. Os cartões de estudante são pré-selecionados pela extensa documentação necessária para se matricular em uma universidade. Esta informação é rotineiramente relatada ao estado de uma forma ou de outra. Esses IDs semiprivados podem ser uma prova de princípio, mas não são de livre mercado ou privados.

A agorista Sunni Maravillosa especula sobre como seria a identidade de livre mercado em seu ensaio “ID without Big Brother”, na antologia *National Identification Systems: Essays in Opposition*:

> "Se um indivíduo deseja um documento de identidade que atribua um determinado rótulo a ele, ele tem várias empresas para escolher. IDs R Us é uma rede nacional que possui requisitos mínimos para tal identificação, e oferece atendimento rápido a preços baixos. No entanto, por ter requisitos mínimos, seu histórico de segurança não é tão bom e muitas empresas não confiam muito em seus IDs. O emissor de ID de autenticação mais bem-sucedido é o Spooner's Identity Emporium. Essa empresa também tem requisitos mínimos para identificação apenas de nome de baixo nível, mas dá a etapa adicional de verificar o histórico do candidato à identificação com esse nome, bem como a reputação daqueles que garantem o candidato à identificação. A empresa publica uma lista mensal em seu site – geralmente uma lista muito curta, devido ao seu processamento cuidadoso – de indivíduos cuja identidade foi revogada, juntamente com o motivo da revogação [...] Claro, se um indivíduo não gostar dos requisitos de uma empresa, ela está livre para usar outra [...]"

A maioria das empresas teria cuidado com a precisão porque qualquer pessoa fraudada por um documento falso pode entrar com uma ação legal. Eles também teriam cuidado com a privacidade do cliente, pois a discrição seria a chave para a comercialização de seu ID. Se os IDs emitidos pela empresa facilitarem a fraude ou se as informações do cliente vazarem, a publicidade por si só prejudicaria ou arruinaria a reputação da empresa; as empresas de identidade de livre mercado viveriam e morreriam com base em suas reputações.

O segundo serviço que a ID de livre mercado oferece aos indivíduos é a *certificação*. Cartas de recomendação atestam o caráter, a educação e as habilidades específicas do portador. As empresas provavelmente cooperariam umas com as outras no fornecimento de tais cartas. Maravillosa oferece um exemplo hipotético:

> Os bancos emitem "credenciais de crédito", que se baseiam no histórico de crédito de um indivíduo ou empresa com o banco, para que outro indivíduo ou instituição esteja con-

> vencido de que a entidade em questão é diferente de inadimplência em um empréstimo ou outro acordo de crédito até um determinado valor.

Novamente, a versão cripto desse serviço é uma recomendação online pessoal de uma figura confiável sobre um estranho. Alternativamente, o estranho poderia apontar para documentos de certificação – talvez artigos acadêmicos que ele escreveu sobre assuntos relevantes. Sua própria reputação pode ser uma identificação de certificação.

Algumas formas de ID atual executam uma função semelhante. Os diplomas universitários supostamente certificam um nível de educação e inteligência; uma carta de referência de um empregador descreve os hábitos de trabalho louváveis de um ex-funcionário; a participação em organizações profissionais ou de caridade sugere o caráter e as habilidades sociais de uma pessoa.

Há uma desvantagem marcada para muitas certificações atuais, no entanto. Uma delas: as licenças e diplomas estatais frequentemente substituem os métodos de certificação do livre mercado. Tudo, de neurocirurgia a tranças de dreadlocks, exige licenças, e estas tendem a substituir a reputação como medida de valor. Um exemplo: Um curandeiro não tradicional é bem conhecido por sua habilidade, mas não consegue obter uma licença. Sua reputação é gigantesca, mas os médicos locais bloqueiam o processo de licenciamento para eliminar a concorrência. O curandeiro é incapaz de tratar as pessoas sem o risco de ir para a cadeia. Diplomas exigidos pelo estado – mesmo que tenham valor, o que é cada vez mais duvidoso – são barreiras para aqueles que são talentosos, mas não sancionados pelo estado. Desta forma, o estado desvaloriza ou nega o valor da reputação.

O terceiro propósito da ID de livre mercado é *autorizar* ações específicas. As cartas podem atribuir direitos limitados ao portador. Um escritório de advocacia pode atribuir um poder limitado a um de seus advogados para que ele possa resolver um caso em nome de um cliente.

Objeções ao ID de livre mercado

Surgem objeções à identificação de livre mercado. Diz-se que os métodos de identificação são antiquados, não fornecem anonimato real

e não têm uniformidade. Além disso, estabelecer uma reputação é um processo lento em um mundo em rápida evolução.

Antiquado. Alguns modelos de identificação podem estar ultrapassados. Mas o remédio mais seguro para isso é abrir o campo e deixar o mercado inovar. Os IDs mais antiquados são os produzidos pelo estado estagnado.

Sem anonimato. O objetivo principal da identificação inicial era verificar a identidade, não tornar o anonimato. E ainda há uma demanda de livre mercado para verificar a identidade. Há valor no anonimato; há valor em ser conhecido. O valor depende de se o indivíduo é capaz de escolher livremente entre os dois.

Sem uniformidade. Outra palavra para "sem uniformidade" é "diversidade", e é uma das vantagens extremas do ID de livre mercado porque dá escolha. A identidade do governo é homogeneizada porque o objetivo é impor a conformidade com as leis e os requisitos de relatórios. Quando o ID atende a indivíduos, sua forma é ditada por suas necessidades e preferências, não pelo estado.

Lento para estabelecer confiança ou reputação. Este é um mundo corrido. Mas o fato de que uma reputação ou um negócio pode levar tempo e trabalho duro para se estabelecer dificilmente é uma crítica. Conquistas que valem a pena levam tempo e trabalho duro.

A opção nuclear do estado no armamento de dados

> "A privacidade inclui a capacidade de manter as coisas em segredo do governo. Posso estar mantendo em segredo minha fraqueza por álcool, heroína, jogos de azar ou pornografia e, assim, impedir que o governo interfira para me proteger de mim mesmo. Se você vê o governo como um super ser benevolente cuidando de você – um tio sábio e gentil com uma longa barba branca – você vai e deve rejeitar muito do que estou dizendo. Mas o governo não é o Tio Sam ou um rei filósofo. O governo é um conjunto de instituições através das quais os seres humanos agem para fins humanos. Sua característica especial – o que diferencia a ação política das outras maneiras pelas quais tentamos obter o que queremos – é que o governo pode usar a força para fazer as pessoas fazerem coisas."
> – David Friedman

O governo não é um tio sábio e gentil. É uma instituição de interesse próprio ocupada por seres humanos com paixões humanas, especialmente por poder, riqueza, status, moralização e vingança. Atualmente, os usuários de cripto têm motivos para serem particularmente privados. Uma notícia recente declara: “A NSA rastreia usuários de Bitcoin desde 2013, novos documentos de Snowden são revelados”. Muita cautela tanto online quanto offline não é paranoia quando eles de fato estão atrás de você.

Uma manchete de 6 de fevereiro de 2018 na revista *Reason* alerta: “Os governos odeiam Bitcoin e dinheiro vivo pelo mesmo motivo: eles protegem a privacidade das pessoas”. O artigo a seguir deriva de uma citação do secretário do Tesouro dos EUA, Steve Mnuchin: “Uma das coisas em que trabalharemos muito de perto com o G-20 é garantir que isso não se torne as contas bancárias numeradas na Suíça”. Mnuchin rejeita as criptos descentralizadas como sistema de pagamento, investimento ou poupança porque não podem ser facilmente rastreadas pelo governo. A crítica de Mnuchin confirma que as criptomoedas são um bem positivo para os indivíduos, não apenas porque os empodera, mas também porque os protege de estatistas como ele.

Os ataques de privacidade em todo o mundo ficarão rapidamente mais agressivos. Os dados estão sendo transformados em armas em um ritmo assustador, criando uma corrida acirrada entre privacidade e totalitarismo. Estados estão desenvolvendo novas maneiras de usar bancos de dados para reprimir as oportunidades e atividades de pessoas que fazem escolhas “erradas” ou que têm pensamentos “errados”.

Uma manchete na Reuters dizia: “China barrará pessoas com mal ‘crédito social’ de aviões e trens”. O crédito social (*xinyong*) é um conceito moral de longa data dentro da tradição chinesa, que indica o nível de honestidade e confiabilidade de uma pessoa. O governo chinês agora estende esse conceito moral para incluir lealdade ao estado e honestidade social ou política; atribui uma classificação oficial a cada pessoa. Então, o controle social extremo é imposto àqueles com pontuações baixas, negando-lhes “privilégios”, como viagens e educação. Os crimes de crédito social incluem usar bilhetes vencidos para embarcar em um trem ou fumar enquanto estiver nele, comprar muito álcool, assistir pornografia, devolver uma bicicleta alugada com atraso, “não comparecer a um restaurante sem cancelar a reserva, trapacear em jogos online, deixando avaliações falsas de produtos, e atravessar a rua fora da faixa.”

As ofensas triviais podem parecer intrigantes ou até engraçadas, mas servem a um propósito importante para o Estado e horripilante para os indivíduos. As ofensas triviais dão ao Estado um cheque em branco para reprimir dissidentes, opositores políticos ou outros "indesejáveis", porque praticamente todos cometem infrações menores como parte da vida cotidiana. Como Beria disse uma vez: "Mostre-me o homem, eu lhe mostrarei o crime". O governo chinês agora pode escolher quem deseja converter em não-pessoa, impedindo-os de viajar e outras interações sociais. A estratégia é semelhante à descrita no livro *Three Felonies a Day*, segundo a qual todos que violam a autoridade do estado são vulneráveis a acusações criminais por um ou outro delito. Todo mundo é vulnerável aos ataques do estado. Esse perigo também fornece um grande incentivo para que as pessoas obedeçam absolutamente e não chamem a atenção para si mesmas. Isso é verdade na China. É cada vez mais verdade em muitas nações.

O conceito de crédito social não é exclusivamente chinês. Nos EUA, os passaportes são negados àqueles que estão suficientemente atrasados no pagamento de pensão alimentícia ou de impostos, e ex-criminosos têm dificuldade em viajar para o exterior. Os estrangeiros que disserem a um guarda de fronteira dos EUA que fumaram maconha, independentemente de o evento ter ocorrido em um local onde era legal ou não, terão sua entrada recusada. *Global News*, um portal de notícias canadense, explica: "eles são [...] instruídos a voltar para o Canadá e informados de que são inadmissíveis pelo resto da vida. Esta é uma proibição vitalícia." Enquanto isso, direitos constitucionais como a posse de armas estão sendo negados por uma lista cada vez maior de razões.

O apetite voraz do governo pelos dados exigidos pelo controle social está crescendo. O Cloud Act tornou-se lei federal em 2018, por exemplo. A lei permite que a aplicação da lei federal obrigue as empresas de tecnologia sediadas nos EUA a fornecer dados armazenados em servidores, independentemente de onde os dados estão armazenados. Ele retira os direitos da Quarta Emenda contra busca e apreensão irracionais, permitindo que os EUA celebrem acordos de compartilhamento de dados com países estrangeiros e ignorem os tribunais dos EUA. Os usuários-alvo podem nunca saber do mandato.

As pessoas precisam escolher sua abordagem à privacidade e se preparar.

O que você deveria fazer?

As estratégias variam de pessoa para pessoa, porque são baseadas em variáveis como personalidade e circunstância. Existem muitos caminhos para a privacidade, não apenas um.

Antes de responder "O que você deve fazer?", algumas distinções são úteis. Todas as informações não são iguais, e criptografar tudo pode chamar atenção indesejada. Você pode considerar criptografar apenas informações importantes para sua liberdade, riqueza e bem-estar. Todo mundo tem pelo menos três tipos de dados pessoais. Primeiro, há dados que devem ser amplamente divulgados, como um currículo de emprego. Esta informação requer marketing, não privacidade. Em segundo lugar, há fatos que são inofensivos de divulgar, como uma cor favorita ou uma preferência por batatas fritas. A divulgação pode atrair solicitações indesejadas de negócios, mas esses aborrecimentos não comprometem direitos. Terceiro, há fatos que os maus agentes podem usar contra você. Os dados financeiros são um excelente exemplo. Este é o ponto em que a privacidade se torna um mecanismo de sobrevivência.

A próxima distinção é o terreno bem trilhado da privacidade versus anonimato versus pseudônimo. Vou pisar nessa questão mais uma vez e brevemente.

Privacidade é o ato de manter dados pessoais ou atividades para si mesmo em sua totalidade ou para qualquer que seja o seu nível de conforto. Qual é o seu nível de conforto?

O anonimato é a estratégia de tornar o conteúdo transparente, mas ocultar os Nomes Verdadeiros. Rick Falkvinge, fundador do primeiro Partido Pirata, elabora:

> "O exemplo típico seria se você deseja denunciar abuso de poder ou outras formas de crime em sua organização sem arriscar a carreira e a posição social desse grupo, e é por isso que normalmente temos leis fortes que protegem as fontes da imprensa livre. Você também poderia postar esses dados anonimamente online por meio de uma VPN, da rede de anonimização TOR ou de ambos. Este é o equivalente análogo da carta de denúncia anônima, que tem sido vista como um procedimento padrão em nossas checagens e avaliações."

O pseudônimo é a estratégia de usar um nome fictício em vez de um Nome Verdadeiro. É o anonimato adquirido pelo disfarce. A pseudonimidade não é um fenômeno recente. Os influentes *The Federalist Papers* (1787-1788) foram escritos por Publius – um pseudônimo coletivo que abrange James Madison, Alexander Hamilton e John Jay. Os historiadores ainda discordam sobre quem escreveu algumas das peças; isso atesta a eficácia do pseudônimo.

As táticas mais eficazes para proteger dados online podem ser tecnológicas, mas este livro não as aborda, exceto de passagem. Em vez disso, ele aponta para estratégias ou hábitos de privacidade que são usados há décadas, se não há séculos. Alguns deles serão familiares. O objetivo não é promover material novo ou revolucionário; é conscientizar as pessoas a pensar em como manter a privacidade.

Eles foram atualizados para focarem nas criptomoedas. Aqui está uma amostra de algumas técnicas básicas e eficazes:

Ofuscar ou "esconder à vista de todos". Seja tão discreto ou sutil em suas ações externas e aparência que seja quase imperceptível. Misture-se e torne-se invisível. Às vezes, a ofuscação envolve a participação em locais tão cheios de "ruído" que um bisbilhoteiro acha difícil distinguir seu sinal de qualquer outro. O cerne desta estratégia é evitar chamar atenção para si mesmo. Quando você fizer coisas "notáveis", como pedir a derrubada do sistema bancário central, faça-o sob um pseudônimo. Sob seu Nome Verdadeiro, seja cauteloso.

Evite corretoras centralizadas e outros centros de compartilhamento de dados. Esta é uma versão atualizada para usuários de cripto do conselho de evitar centros de coleta de dados conectados ao estado, como os bancos centrais. Se você deseja que o estado tenha todos os seus dados financeiros, basta enviá-los por correio para as agências estaduais.

Proteja tudo com senha e fique livre de vírus. Uma senha é como uma fechadura em uma porta que dificulta a entrada de malfeitores. Evite vírus e malwares através dos quais hackers podem atacar seus dados e roubar sua identidade. Nunca abra arquivos não solicitados em e-mails; nunca baixe arquivos de sites desconhecidos ou inseguros. Execute um programa antivírus competente e prefira navegadores que resistam a penetrações, como os usados em Linux.

Encontre maneiras discretas de sacar. O veterano das criptos Kai Sedgwick escreve: "As transações Bitcoin são semianônimas: todas as transações na blockchain são transmitidas publicamente e visíveis por

toda a eternidade, mas o proprietário de cada carteira é desconhecido. Vincular endereços a identidades do mundo real agora é relativamente fácil para os poderosos, porque todos precisam sacar em algum lugar, e isso geralmente envolve vincular endereços de Bitcoin a contas bancárias." Não use terceiras partes confiáveis para sacar. Na medida do possível, lide com as pessoas individualmente ou por meio de corretoras descentralizadas que facilitam a compra e a venda peer-to-peer. Seja inventivo. Procure locais que troquem criptomoedas por gift-cards em lojas nas quais você faz compras regularmente, incluindo mercearias.

Escolha um mecanismo de pesquisa que respeite a privacidade. Muitos mecanismos de pesquisa registram históricos de navegação e os usam para segmentar anúncios ou gerar receita vendendo-os. Outros, como o DuckDuckGo, não rastreiam dados pessoais.

Use uma moeda de privacidade. Existem dezenas dessas moedas e mais estão chegando porque a privacidade está em demanda. O fundador da Zcash explica a filosofia por trás de sua moeda de privacidade. "Acreditamos que a privacidade fortalece os laços sociais e as instituições sociais, protege as sociedades contra seus inimigos e ajuda as sociedades a serem mais pacíficas e prósperas [...] Uma tradição robusta de privacidade é uma característica comum em sociedades ricas e pacíficas, e a falta de privacidade é frequentemente encontrada em sociedades com dificuldades e fracassadas".

Nunca dê mais informações do que o necessário. Nunca forneça informações, especialmente por escrito, sempre que a recusa ou o silêncio for uma opção. Se um formulário é obrigatório, preencha o menor número de espaços em branco possível da forma mais confusa possível. Desconfie de qualquer empreendimento conectado às criptomoedas que exija mais do que informações mínimas para adquirir o serviço ou bem que está sendo oferecido. Ninguém nas criptos precisa saber seu número de previdência social, mesmo os últimos quatro dígitos. Sempre pergunte a quem solicita informações "por que" elas são necessárias e quais os usos que farão delas. Decida com antecedência quantos dados você está disposto a divulgar e de que forma.

Seja cauteloso em fóruns públicos. Fóruns públicos, como Facebook ou Twitter, são monitorados e explorados por governos e corporações; eles também são monitorados por criminosos e pessoas maliciosas que guardam rancor. Fóruns públicos são pontos de coleta de dados pessoais, mesmo que uma pessoa pense que está postando anonimamente.

Se a mídia social for necessária por motivos profissionais, use-a ao mínimo e apenas por motivos profissionais. Nunca publique nada nas redes sociais que você não colocaria na primeira página do *New York Times*.

Tenha cuidado ao registrar informações. Não anote chaves privadas, por exemplo, sem ter um local seguro e não divulgado para armazená-las. Não faz sentido criptografar dados online se o mesmo informativo estiver em forma cursiva na mesa da cozinha.

Use apenas conexões Wi-Fi seguras. É comum as pessoas se conectarem ao Wi-Fi gratuito na Starbucks e em outros locais, mas não há como saber quem pode estar ouvindo seu tráfego de internet. Se você precisar usar Wi-Fi inseguro, não transmita dados pessoais e use um serviço VPN para criptografar dados pessoais.

Minta ao estabelecer perguntas de segurança de senha. "Qual é o nome de solteira da sua mãe?" Com essas informações, alguém malicioso pode invadir suas contas bancárias e, talvez, roubar sua identidade. Não responda a esta ou a outras perguntas de "identificação" padrão com sinceridade. Tenha uma resposta falsa padrão que você não use em formulários oficiais ou importantes que sejam seguros. Sobre esses, diga a verdade.

As precauções rudimentares anteriores destinam-se a formar o hábito da privacidade. Muitas pessoas têm o hábito de revelar, de dizer a verdade reflexivamente. Um hábito nada mais é do que uma resposta automática que resulta de um padrão de comportamento estabelecido. Pode ser difícil quebrar o hábito da divulgação e substituí-lo pela discrição, mas é necessário fazê-lo. Nunca minta para um amigo, mas não entregue a um estranho as chaves da sua identidade.

O governo está indo atrás das criptos, o que significa que ele está investigando os usuários. Seu ataque na linha de frente será um ataque à privacidade, porque a privacidade é a espinha dorsal da criptografia como ferramenta de liberdade. Agora é a hora de aumentar a vigilância. Parafraseando a comediante Lily Tomlin: "Não importa o quão paranoica eu fique, nunca é suficiente para acompanhar o ritmo".

A privacidade pode ser a defesa da linha de frente da liberdade individual, mas a descentralização é a condição social sob a qual a privacidade prospera. Ninguém pode ou deve dizer aos indivíduos qual estratégia específica usar. Mas, se você valoriza privacidade e segurança, mantenha a privacidade e se descentralize.

SEÇÃO TRÊS

Descentralização

Descentralização no Núcleo da Cripto-Liberdade

> "Muitas pessoas descartam automaticamente a moeda eletrônica como uma causa perdida por causa de todas as empresas que faliram desde a década de 1990. Espero que seja óbvio que foi apenas a natureza centralmente controlada desses sistemas que os condenou. Acho que esta é a primeira vez que estamos tentando um sistema descentralizado e não baseado em confiança."
> – Satoshi Nakamoto

Apesar do incrível sucesso das criptomoedas, a questão de saber se o livre mercado pode estabelecer um sistema monetário viável ainda surge. Muitas vezes é sugerido que a cripto é viável apenas porque existe em paralelo com a moeda fiduciária, com a qual é conversível e sobre a qual se baseia. Mas será que a instituição do dinheiro, em última análise, exige supervisão confiável de terceiras partes e o envolvimento do estado? (Uma instituição é uma lei, prática ou costume estabelecido dentro de uma sociedade).

A questão pode ser reduzida a uma mais fundamental: como surge qualquer instituição dentro da sociedade e como ela declina? A resposta está dentro dos conceitos de descentralização e centralização.

O que é Centralização? O que é Descentralização?

A centralização concentra o controle de uma atividade ou organização sob uma única autoridade para coordenar os resultados. Em termos de monopólio monetário, a atividade é a sociedade; a autoridade é o estado que coordena o fluxo de finanças com o objetivo declarado de produzir uma economia eficiente e produtiva. Outro termo para o controle centralizado da sociedade é "engenharia social". O estado aplica as teorias da ciência social à gestão de seres humanos para controlar o posicionamento e funcionamento de cada um. O controle social visa alcançar uma sociedade que seja justa ou efetiva de acordo com a visão dos responsáveis.

Nem toda centralização dispensa a escolha individual. Empresas privadas podem centralizar-se sob uma equipe de gerenciamento para

aumentar os lucros, por exemplo. Quando o fazem, muitas vezes são chamadas de corporações. A diferença crucial entre esse cenário e a centralização estatal é que as empresas são voluntárias e os indivíduos envolvidos são livres para ir embora e se juntar a um concorrente. Com o controle social, os indivíduos não têm escolha. Afastar-se significa infringir a lei, e não há concorrente.

A descentralização é a difusão do poder de uma autoridade central para suas unidades constituintes. Na arena política, isso significa passar o controle do nível nacional para o local. A discussão da descentralização geralmente começa e termina na esfera política, com o poder ainda investido em uma autoridade coordenadora. Um governo local pode ser melhor do que um remoto porque é mais responsivo à comunidade, mas o ponto final lógico da descentralização é o indivíduo, que é o alicerce de toda a sociedade e sua unidade constituinte mais básica. Esse arranjo é tanto um método quanto um objetivo. O método é o empoderamento do indivíduo. O objetivo é uma sociedade saudável, na qual cada membro faça suas próprias escolhas de acordo com seu próprio interesse.

A centralização está tão entrelaçada no tecido da cultura que muitas pessoas acreditam ser necessária para o funcionamento da sociedade. Escolas públicas, bancos centrais, sistema judiciário, obras públicas, estradas governamentais, tarifas … A maioria das pessoas não consegue visualizar a sociedade através de qualquer outra lente que não a do controle estatal centralizado; é tudo o que conhecem e tudo o que aprenderam.

Ao longo da maior parte da história, a sociedade foi vista como o resultado do projeto de alguém. O designador pode ser Deus, um chefe tribal, um monarca, um comitê de socialistas ou comunistas, uma equipe de especialistas ou alguma outra entidade que também era o estado, só que com outro nome. A sociedade era vista como uma construção artificial criada e gerida pelas autoridades. A sociedade era considerada dependente de uma autoridade coordenadora para sua lei, moralidade e prosperidade.

Em sua obra de três volumes *Law, Legislation and Liberty*, o teórico social Friedrich Hayek se refere a essa posição como “racionalismo construtivista”. Uma crença construtivista central é que o homem pode e deve inventar conscientemente instituições sociais, como a lei, através da aplicação da razão e da ciência social. Hayek argumenta vigorosamente contra essa perspectiva, alegando que os construtivistas não compreendem o processo pelo qual as instituições da sociedade surgem e

evoluem. De fato, ele acredita que a abordagem construtivista é antitética com o processo real, e dificulta as instituições sociais que deveriam evoluir em vez de seguir um plano. Em uma palestra no Memorial do Nobel de 1974 intitulada “The Pretense of Knowledge”, Hayek expressa uma objeção epistemológica básica ao construtivismo – isto é, uma objeção baseada em uma teoria do conhecimento humano. Ele afirma que nenhum comitê pode predizer as escolhas em evolução e os resultados não intencionais de uma massa de pessoas que interagem ao longo do tempo. A preferência humana é muito variável e muda de forma a frustrar todo o planejamento.

Para reciclar uma citação anterior no livro:

> “O reconhecimento dos limites insuperáveis para esse conhecimento deve […] ensinar ao estudante da sociedade uma lição de humildade que deveria protegê-lo de se tornar um cúmplice da batalha fatal do homem para controlar a sociedade – uma batalha que não apenas o fará um tirano sobre seus semelhantes, mas que pode muito bem fazê-lo o destruidor de uma civilização a qual nenhum cérebro designou, mas sim que cresceu dos esforços livres de milhões de indivíduos.”

Contemporâneo de Hayek, Ludwig von Mises chega à mesma conclusão de um ângulo menos epistemológico e mais econômico em sua obra-prima *Human Action*:

> “A ação humana origina a mudança. Na medida em que há ação humana, não há estabilidade, mas alteração incessante […] Os preços do mercado são fatos históricos expressivos de um estado de coisas que prevaleceu em um instante determinado do processo histórico irreversível. […] No imaginário e, claro, estado irrealizável de rigidez e estabilidade, não há mudanças a serem medidas. No mundo atual de mudanças permanentes, não há pontos fixos […]”

Tanto Hayek quanto Mises acreditam que o conhecimento buscado pelos construtivistas é inatingível. Não é possível planejar a dinâmica de amanhã com base na de ontem porque as preferências das pes-

soas e outras circunstâncias são imprevisíveis, mesmo pelas pessoas envolvidas; suposições são possíveis, mas o conhecimento não é. Mesmo uma coisa pequena, como o preço do pão ontem, não dá conhecimento do preço do pão amanhã, porque pode disparar devido à falta de farinha ou a uma mudança nas prioridades das pessoas.

Usar uma foto estática da sociedade de ontem para projetar o futuro vai contra um princípio básico da ação humana e da natureza humana: mudança inevitável. A mudança inevitável é uma diferença fundamental entre os seres humanos e os objetos físicos examinados pelas ciências exatas sobre as quais os construtivistas baseiam sua teoria social. Um cientista pode aprender tudo o que precisa saber para prever o comportamento de uma rocha porque a rocha é estática ao longo do tempo. A água continua a ter a mesma estrutura molecular e continua a ser definida por constantes, como a lei da gravidade, por exemplo. Mas a sociedade não consiste em objetos invariáveis. O comportamento dos seres humanos é baseado na alteração de preferências, emoções e respostas psicológicas que podem ser conflituosas ou ocultas até mesmo das pessoas que estão agindo. Os seres humanos não podem ser categorizados, empilhados e obrigados a obedecer às leis da ciência. A sociedade consiste em indivíduos imprevisíveis, que reagem a mudanças nas circunstâncias. Não são rochas ou água.

Há duas maneiras de os teóricos sociais abordarem a desobediência do homem imprevisível. Eles podem aceitar a natureza dos seres humanos e trabalhar suas teorias em torno dela, ou podem tentar mudar a natureza do homem para que ele se adeque às teorias deles.

Os construtivistas escolhem a segunda opção, com o novo Homem Soviético ou Pessoa Soviética sendo uma manifestação de suas teorias. O novo homem soviético foi considerado a evolução lógica dos seres humanos sob o regime comunista. Em seu livro *The Mass Psychology of Fascism* (1933), o psicanalista alemão Wilheim Reich pergunta: “O novo sistema socioeconômico se reproduzirá na estrutura do caráter das pessoas? Se sim, como? Suas características serão herdadas por seus filhos? Será ele uma personalidade livre e autorregulada? Os elementos de liberdade incorporados à estrutura da personalidade tornarão desnecessárias quaisquer formas autoritárias de governo?”

A natureza humana, assim como a sociedade, seria reconstruída por aqueles que estão no poder. O novo homem soviético era um arquétipo ou ser humano ideal com características específicas que seriam pro-

jetadas e que evoluiriam a partir do comunismo. A nova natureza humana seria compartilhada por todos os povos soviéticos, independentemente de fatores como diferentes origens culturais ou étnicas. As características comunistas incluíam altruísmo, entusiasmo pelo comunismo, saúde física, coletivismo e disciplina. Também haveria uma nova mulher soviética, como o mundo nunca tinha visto antes – abnegada e dedicada aos ideais revolucionários.

Em contraste, Hayek trabalha desapaixonadamente com a natureza humana como ela se mostra a ele: interessada por si mesma e individualista. Ele vê a engenharia social como sendo mais que meramente impossível: é também tremendamente destrutiva, porque é a antítese de uma sociedade natural e destrói as instituições liberais que evoluíram para servir aos indivíduos, e não ao estado.

Hayek conhecia em primeira mão as terríveis consequências do planejamento central. Ele havia testemunhado a devastação do liberalismo clássico por duas guerras mundiais, mas especialmente pela Primeira Guerra Mundial, que despedaçou os moldes do livre mercado. O governo em tempo de guerra havia fixado o controle centralizado sobre o setor privado para garantir o fluxo de armamentos e outros bens "necessários". O dinheiro havia sido drasticamente inflacionado e reduzido em valor para pagar por maciços aumentos militares. A guerra estrangulou o fluxo do livre comércio, que os liberais clássicos pensavam ser um pré-requisito para a paz entre as nações, bem como para a prosperidade dos indivíduos. Hayek viu como a máquina centralizadora do estatismo do século XX destruiu a promessa do liberalismo clássico do século XIX.

Em refutação ao construtivismo, os economistas austríacos descrevem como as instituições em uma sociedade saudável surgem espontaneamente. As descrições geralmente começam com modelos simplistas para ilustrar um princípio básico ou ponto – o jeito como um caminho é forjado através de um campo, por exemplo. Uma pessoa toma o caminho mais curto através de um campo coberto de mato, e sua passagem deixa um rastro tosco de grama pisada para trás. Por uma questão de conveniência, a próxima pessoa que cruza o campo usa o caminho áspero, que fica mais claramente estabelecido como resultado. Cada pessoa que cruza posteriormente contribui para tornar o caminho mais visível e mais fácil de percorrer. Ninguém constrói o caminho intencionalmente ou como um serviço a outras pessoas; é simplesmente do interesse de cada pessoa usar a rota mais fácil através do campo. No

entanto, o reforço auto interessado do caminho beneficia a todos os que percorrem o campo depois.

Uma das primeiras obras de Mises, *Nation, State and Economy* (1919) analisa o quanto fenômenos sociais mais complexos – como a linguagem – também foram consequências não intencionais de interações individuais. Nenhum comitê ou autoridade central decidiu inventar a fala humana ou publicar um dicionário, muito menos projetar uma linguagem específica como o inglês. De maneira completamente alheia ao benefício da lei, os indivíduos começaram a se comunicar para obter o que queriam uns dos outros. Os sons emitidos gradualmente se tornaram mais redefinidos e variados, mesmo quando os significados de sons específicos se tornaram mais amplamente reconhecidos. A linguagem evoluiu.

Hayek desenvolve um sistema similarmente sofisticado de teoria social para explicar como todas as instituições da sociedade evoluem naturalmente de baixo para cima – das interações voluntárias e não planejadas dos indivíduos – e não de cima para baixo – de especialistas ou poderosos que impuseram sua vontade. As instituições naturais, sustenta Hayek, são os resultados coletivos, mas não intencionais, da interação humana: "é resultado da ação humana, e não da projeção humana". Mesmo fenômenos sociais complexos – como a escrita, a religião ou o dinheiro – são consequências não intencionais da interação humana. A suposta eficiência dos programas governamentais empalideceu em comparação, para dizer o mínimo.

Os construtivistas contra-argumentam que uma sociedade não planejada é caótica e esbanjadora. Com conhecimento suficiente e uma abordagem científica, eles acreditavam que uma sociedade perfeitamente eficiente poderia ser projetada. Sem excedentes, sem escassez, sem desperdício, sem desemprego. Os mercados de ações não entrariam em colapso e as moedas não flutuariam, exceto quando deveriam fazê-lo. A sociedade poderia ser construída de modo que seus membros caminhassem em uníssono em direção aos mesmos objetivos sociais supostamente desejáveis, assim como haviam marchado em uníssono como soldados rumo à vitória na guerra.

A resposta de Mises aos construtivistas reformularia o conceito de individualismo.

O Novo Individualismo Austríaco

Uma nova concepção de individualismo surgiu em resposta a uma teoria que acompanhava o construtivismo. O holismo social tornou-se popular no início do século XX. O holismo social afirma que os sistemas devem ser vistos como totalidades e não como coleções de suas partes, e a dinâmica de um todo difere da soma de suas partes. Em suma, o coletivo é maior e diferente das unidades que o compõem. Uma análise holística da sociedade geralmente começa com um estudo do coletivo, e não do indivíduo, e assume que o comportamento do indivíduo é determinado pelo coletivo. O comportamento individual é definido pelas categorias e propriedades da classe que compõem seu contexto. A sociedade é mais do que a soma total dos indivíduos que a constituem.

Economistas austríacos afirmam o contrário. A sociedade resulta de e é explicada pelo comportamento dos indivíduos que, coletivamente, *são* a sociedade. A sociedade não tem existência independente de seus membros individuais, todos os quais agem em seu próprio interesse. No entanto, o interesse próprio não é equivalente ao egoísmo, pois os atos tradicionalmente altruístas – doar para a caridade, ajudar o próximo, sacrificar-se pela família – são frequentemente vistos pelos indivíduos como um comportamento que enriquece a vida. No que parece um paradoxo para alguns, atos tradicionalmente altruístas são muitas vezes realizados como uma questão de interesse próprio.

Os marxistas acusam aqueles que reduzem a sociedade a indivíduos de serem atomistas; isto é, diz-se que eles fragmentam a sociedade em unidades desconexas e isoladas, de modo que a sociedade não existe verdadeiramente. Em resposta, alguns marxistas chegam ao ponto de afirmar que é o indivíduo, e não a sociedade, que é a verdadeira abstração. Ou seja: os indivíduos não existem sem uma sociedade envolvente, que os defina e os construa. Mises fez uma observação sobre essa posição: “A noção de um indivíduo, dizem os críticos, é uma abstração vazia. O homem real é necessariamente sempre um membro de um todo social”.

Karl Marx argumenta um ponto semelhante a este usando um cenário de Robinson Crusoé, que é uma maneira popular de construir um argumento sobre a natureza humana a partir de seus fundamentos absolutos: o homem isolado. Um indivíduo que nasce e é abandonado em uma ilha deserta, afirma Marx, será mais um ser humano em potencial

do que um ser humano real. (Alguns socialistas, como Hegel, argumentam que o próprio homem era uma abstração.) Marx faz uma distinção entre a "natureza humana em geral" e "natureza humana modificada" por períodos históricos de épocas. Existem dois tipos de impulsos humanos: aqueles que são fixados, como a fome, e aqueles que "devem sua origem a certas estruturas sociais e a certas condições de produção e comunicação". O ponto de Marx é que, além de características inerentes ao instinto, a natureza humana é uma construção social definida pelo contexto social; a sociedade cria a essência humana de seus membros individuais. Isso significa que a sociedade poderia construir o que Marx considera ser o tipo certo de humanidade – como o novo homem soviético – caso as instituições da sociedade fossem totalmente orientadas para alcançar esse objetivo.

Os liberais clássicos argumentam o contrário: uma pessoa criada isoladamente ainda será um ser humano realizado com características humanas que vão muito além de um impulso para as necessidades básicas de sobrevivência. Por exemplo: Crusoé terá uma escala de preferências que os economistas chamam de utilidade marginal decrescente, e ele agirá para atingir primeiro a mais alta; ele obterá água para beber antes de se banhar. Ele terá curiosidade e capacidade de sentir tristeza. Sem interação social, grandes partes de seu potencial nunca se desenvolverão, é claro, mas isso não o torna menos humano ou vazio de vontade e personalidade individuais. Os coletivos oferecem incentivos para comportamentos específicos, mas não definem a humanidade dos indivíduos. São os seres humanos e sua natureza inata que definem o coletivo. Sob a análise de Mises, esse argumento simples evolui para uma nova e abrangente abordagem do individualismo.

Como uma teoria social geral, o individualismo significa a defesa da liberdade individual em oposição ao poder de um coletivo, especialmente o estado. Como uma questão pessoal, significa que as pessoas fazem suas próprias escolhas pacíficas e assumem a responsabilidade por elas. Embora um individualista às vezes seja caracterizado como solitário, o oposto geralmente é verdadeiro, porque os seres humanos são animais sociais – eles anseiam por interação quase tanto quanto por comida e abrigo. A cooperação e o comércio são a realização do individualismo, porque permitem que o indivíduo expresse preferências e satisfaça necessidades. "Uma vez percebido que a divisão do trabalho é a

essência da sociedade", observa Mises, "nada resta da antítese entre indivíduo e sociedade. A contradição entre o princípio individual e o princípio social desaparece".

Um conceito central da filosofia individualista de Mises é a "praxeologia" – uma palavra [práxis] que significa "obra" ou "ação", e que deriva do grego antigo. Seu significado moderno é "o estudo da ação humana, baseado na crença de que o comportamento humano é proposital em oposição a não intencional ou reflexivo, como piscar". Exceto pelo comportamento reflexivo, as pessoas agem, e o fazem porque é de seu interesse fazê-lo, mesmo que seja apenas para remover aquilo que Mises chama de "sensação de insatisfação". Isso acontece tanto para mudar de cadeira, visando aliviar um músculo dolorido, quanto para investir no mercado de ações para garantir a aposentadoria. Toda ação humana é individual, intencional e auto interessada.
Mises então esboça a teoria mais associada a ele. Sua obra-prima *Human Action* descreve o individualismo metodológico:

> "Primeiro devemos perceber que todas as ações são realizadas por indivíduos. Se examinarmos o significado das várias ações realizadas por indivíduos, devemos necessariamente aprender tudo sobre as ações do todo coletivo. Um coletivo social não tem existência ou realidade fora das ações dos membros individuais. Por exemplo: os indivíduos que compunham uma família interagiam uns com os outros dentro de um contexto específico; a soma dessas interações individuais era o que constituía a abstração 'família'."

Mises usa a ideia não ideológica e neutra do individualismo metodológico para descrever a natureza básica da ação humana, bem como para desconstruir a abstração do estado. Se apenas os indivíduos agem, então tudo o que o estado faz ou é pode ser reduzido a ações tomadas pelos indivíduos que coletivamente constituem o estado. Em um exemplo famoso, Mises explica: "É o carrasco, e não o estado, que executa o criminoso. É o significado dessa ação que simboliza, na ação do carrasco, uma ação do estado". Indivíduos que olham para o carrasco veem o estado, mas apenas porque aceitaram a abstração chamada "o estado" como uma estrutura de compreensão do comportamento do carrasco. Sem o contexto do estado, o carrasco seria visto como um assassino, e não como um instrumento de justiça.

Mises admite prontamente que o carrasco age em relação a outros indivíduos, como os juízes, que também constituem o estado; o carrasco faz parte do sistema penal. Ele também pode agir sob coerção, porque a recusa em executar um criminoso pode causar demissão e dificuldades para sua família. Mas a praxeologia está preocupada apenas com o comportamento de um indivíduo, que é o ponto de partida e a única prova observável da preferência individual. A praxeologia não trata das influências sociais ou psicológicas sobre a ação humana; esse trabalho pertence a "outro departamento". Mises simplesmente afirma que todas as ações são iniciadas e realizadas por indivíduos que agem para promover seus próprios interesses. Explicado de outra forma: não é o estado, mas o carrasco individual que levanta o machado mortal. É o braço do carrasco, e ele não pode escapar da responsabilidade pelas ações que escolhe tomar. (Claro, isso não exonera outros indivíduos envolvidos, como os juízes, por exemplo).

Se apenas os indivíduos agem, então o comportamento coletivo nada mais é do que a soma total das ações e interações dos membros individuais. É comum falar de coletivos ou abstrações como se fossem entidades separadas, que são mais importantes que seus membros. É comum falar dos indivíduos como se agissem e pensassem como um grupo. Quando um homem é preso, por exemplo, o noticiário informa que ele foi apanhado pela polícia. Na realidade, o homem foi algemado por um único policial, e só depois de um único juiz ter assinado o mandado de prisão. Quando ocorre uma batalha, o jornal relata um avanço militar, quando na verdade foram aqueles soldados específicos os únicos a terem de fato avançado. Grupos não agem ou pensam; os indivíduos o fazem; e, às vezes, os indivíduos optam por obedecer a uma autoridade central, que acaba dando a impressão de pensamento coletivo.

O individualismo metodológico soa antissocial para alguns. A impressão também pode ser reforçada pelo uso que Mises faz do exemplo de Robinson Crusoé – o homem isolado – para explicar a praxeologia. No entanto, este uso não sugere que os seres humanos sejam antissociais. Muito pelo contrário. O experimento mental de Crusoé destina-se apenas a remover o fator complicador das relações interpessoais enquanto busca a questão "o que é a ação humana qua ação humana?" É semelhante a um cientista voltando aos princípios fundamentais para entender uma dinâmica. As conclusões de Crusoé são então aplicadas ao mundo real da sociedade.

O *Human Action* explica:

> Se a praxeologia fala do indivíduo solitário, agindo apenas em seu próprio nome e independente dos outros, o faz em prol de uma melhor compreensão dos problemas da cooperação social. Não afirmamos que tais seres humanos autárquicos isolados já tenham vivido, e nem que o estágio social dos ancestrais não humanos do homem, assim como o surgimento dos laços sociais primitivos, tenham se efetivado no mesmo processo. O homem apareceu na cena dos acontecimentos terrenos como um ser social. O homem a-social, isolado, é um constructo fictício. (Nota: Autarquia é a característica da autossuficiência).

A sociedade aumenta o individualismo porque afasta o ser humano do nível animal, permitindo que cada pessoa alcance seu potencial e realize objetivos que seriam impossíveis se buscados de maneira isolada. A interação também é um mecanismo de sobrevivência. A riqueza produzida em conjunto pode ser muito mais abundante do que a riqueza produzida de forma privada, por exemplo, o que deixa todos os envolvidos mais ricos e mais propensos a prosperar. É justamente esse tipo de cooperação que levou a humanidade a dominar o planeta. Os seres humanos são profundamente sociais e as recompensas da sociedade são imensas.

Mises argumenta que os coletivos – como a família ou a sociedade – são abstrações de valor inestimável, pois permitem que as pessoas entendam e descrevam suas interações com outros indivíduos. Os coletivos fornecem o contexto específico para dar sentido à ação individual e à mudança da dinâmica do grupo. Ele explica: “O individualismo metodológico, longe de contestar o significado de tais totalidades coletivas, considera como uma de suas principais tarefas descrever e analisar as origens e as ruínas dessas totalidades, assim como suas estruturas cambiantes e seu funcionamento. E ele o escolhe como o único método adequado para resolver satisfatoriamente esse problema”. O individualismo é a chave para entender os coletivos. É a descentralização aplicada à vida real e cotidiana.

E, ainda assim, se apenas os indivíduos agem, como podem surgir instituições coletivas? A resposta volta ao conceito de ordem espontânea desenvolvida por Hayek e outros.

Ordem Espontânea na Produção Econômica

A análise até agora se concentrou em como as instituições e a sociedade *podem* surgir – arguivelmente, como um sistema saudável deve surgir – em função do livre mercado e da livre associação. A dinâmica é bem fácil de ser descrita se usada como referência uma tribo isolada. Mas será que a estrutura do individualismo pode ser expandida do nível local ao global, a fim de fornecer mecanismos complexos, como o comércio internacional, onde os indivíduos geralmente não se conhecem nem interagem diretamente?

No nível local, a cooperação geralmente é intencional. Os agricultores vendem os produtos para os mercados locais; uma equipe de programadores projeta o melhor e mais recente aplicativo; um hospital coordena os horários dos funcionários, com médicos consultando os pacientes; caminhoneiros entregam mercadorias em determinado endereço; um negócio de startup contrata um especialista em marketing. Estes são contatos intencionais e diretos dentro do contexto limitado de uma sociedade.

Como podem indivíduos, de países estrangeiros, que não se conhecem e nem falam a mesma língua, esperar cooperar na criação de alguma coisa? Por acaso não é necessária uma autoridade suprema para a coordenação de estranhos no comércio global? Se assim for, então a autoridade suprema – isto é, o estado – também é necessária internamente, porque todas as nações modernas vivem ou morrem no comércio global. A exigência de centralização reintroduz o estado como um poderoso e legítimo policial da economia.

Mas o comércio global não requer supervisão. Pode parecer paradoxal dizer que estranhos irão cooperar inconscientemente para benefício mútuo porque é do seu próprio interesse fazê-lo. Mas é isso o que acontece. A cooperação não visa a criação de sociedades ou instituições. Cada participante visa enriquecer-se.

"Eu, o Lápis" é um breve ensaio de Leonard Read, fundador da Foundation for Economic Education. É uma curta história contada a partir da perspectiva de um lápis, que narra sua própria criação. A saga começa com a colheita, mineração e formação de matérias-primas em terras distantes, incluindo cedro, cola, cera, grafite, laca e pedra-pomes. Os trabalhadores estrangeiros vendem quantidades definidas para uma variedade de negócios estrangeiros, e o fazem visando ganhar dinheiro

para alimentar suas famílias. Podem desconhecer o destino ou finalidade das matérias-primas; eles podem não se importar, mas eles o fazem mesmo assim.

As tripulações de navios estrangeiros transportam os materiais para um destino específico, onde os estivadores descarregam os contêineres e os caminhoneiros os transportam para uma fábrica de lápis. Os indivíduos da tripulação e os do cais provavelmente são indiferentes ou ignoram o conteúdo da carga, porque recebem os mesmos salários independentemente da remessa. Até este ponto, todos os envolvidos na fabricação de pré-lápis não se importam com os próprios lápis; eles nem mesmo sabem o papel que desempenham no processo da fabricação dos lápis. Seu propósito é, pura e simplesmente, ganhar a vida.

A matéria-prima chega a uma fábrica de lápis, onde pode começar a cooperação autoconsciente para a criação do lápis. Embora as fábricas de lápis hoje sejam provavelmente automatizadas, isso não diminui a cooperação humana necessária para produzir um lápis. Mesmo as fábricas automatizadas exigem supervisão administrativa, assim como fornecedores de equipamentos, reparadores, zeladores, investidores e uma série de outros indivíduos para produzir um único lápis. No entanto, isso não significa que essas pessoas se conheçam, nem necessariamente que se importem com lápis. O que isso tudo de fato significa é que eles querem lucrar com salários e retornos.

O produto de uma multidão de estranhos que agem apenas segundo seus próprios interesses isolados é um lápis.

Em sua introdução a “Eu, o Lápis”, o economista ganhador do Nobel Milton Friedman escreve:

> Nenhuma das milhares de pessoas envolvidas na produção do lápis executou sua tarefa porque queria um lápis. Alguns deles nunca viram um lápis e não sabem para que serve. Cada um vê seu trabalho como uma forma de obter os bens e serviços que deseja: bens e serviços que produzimos para obter o lápis que desejamos. Cada vez que vamos à loja e compramos um lápis, estamos trocando um pouco de nossos serviços pela quantidade infinitesimal de serviços; os serviços que cada um dos milhares de indivíduos prestaram para conseguir o que queriam, e que acabaram por produzir o lápis.

> É ainda mais surpreendente que o lápis tenha sido produzido. Ninguém sentado em um escritório central deu ordens a essas milhares de pessoas. Nenhum policial militar fez cumprir as ordens que não foram obedecidas. Essas pessoas vivem em países diferentes, falam línguas diferentes, praticam religiões diferentes e podem até se odiar – e ainda assim, nenhuma dessas diferenças os impediu de cooperar para, sabendo ou não, produzir um lápis. Mas como foi que isso pôde acontecer? Adam Smith nos deu a resposta […] há duzentos anos.

A resposta de Smith foi a "mão invisível". O termo é introduzido no livro que Smith considera sua obra-prima: A Teoria dos Sentimentos Morais, e reaparece em sua obra subsequente, A Riqueza das Nações. A Mão Invisível refere-se aos benefícios não intencionais, mas imensos para a sociedade, que fluem de pessoas que agem em seus próprios interesses, especialmente no interesse econômico, da maneira descrita pelo conto "Eu, o Lápis". Quase que invisivelmente, a ordem surge das ações auto interessadas de indivíduos, que cooperam com outros de maneira intencional ou não, consciente ou não. A ordem natural declina quando a interação voluntária é prejudicada pela interferência do estado. Em suma, a liberdade traz civilização e prosperidade; o poder produz conflito e pobreza.

"Eu, o Lápis" e "A Mão Invisível" esclarecem outra confusão que pode advir de discussões de ordem espontânea; ou seja: a definição de ordem espontânea como o "resultado da ação humana, mas não da projeção humana" é um pouco ambígua. Claramente, há uma ordem planejada dentro da cadeia de atividades necessárias para fazer um lápis. Os trabalhadores que coletam as matérias-primas trabalham para uma empresa que tem, projetado, um objetivo específico, e o mesmo vale para os trabalhadores dos navios e das docas. A fábrica é uma máquina altamente projetada.

A frase "o resultado da ação humana, mas não da projeção humana" não nega que a produção requer projeção. "Não da projeção humana" significa que nenhum planejador central organiza e coordena qualquer etapa da produção. Toda a organização e estrutura são fornecidas por aqueles indivíduos que, em diferentes etapas, projetam, gerenciam ou trabalham de maneira independente, dentro de suas próprias etapas, para os empreendimentos que resultam, na soma total dessas

etapas, em um lápis. Sem uma autoridade de supervisão, eles se coordenam e funcionam bem. De fato, uma autoridade supervisora seria um obstáculo à sua eficiência. A frase "o resultado da ação humana, mas não da projeção humana" procura explicar como redes complexas podem surgir da cooperação "não intencional": uma cooperação da qual a vida moderna depende.

"Não da projeção humano" refere-se ao exército de estranhos, cujas ações auto interessadas e ostensivamente descentralizadas entregam, sem a necessidade de intenção, uma variedade impressionante de mercadorias. Eles só precisam agir (e sempre agem) em seu próprio interesse. Como resultado, a pessoa média desfruta hoje de um padrão de vida mais alto do que os nobres no passado, incluindo frutas fora de época e uma magnífica variedade de vinhos para acompanhá-las. A cooperação também une as pessoas em paz, porque elas têm interesse em continuar a lucrar umas com as outras por meio do comércio. Multiplique essa cooperação pelos muitos milhões de interações que criam milhões de produtos e serviços, e a dinâmica coletiva se torna uma cola que mantém as sociedades unidas e permite que o comércio global surja: comércio esse que é o motor da paz.

Até agora, a ordem espontânea foi aplicada à economia – a base da sociedade. Dentro da ordem espontânea, a economia é muitas vezes chamada de cataláxia.

A Cripto Como um Fenômeno Econômico Austríaco

> O Bitcoin é melhor entendido quando visto pela lente conceitual da Cataláxia: os participantes do Bitcoin formam espontaneamente um ecossistema monetário e financeiro descentralizado, escolhendo coletivamente o Bitcoin como meio de troca e reserva de valor. O Bitcoin é uma demonstração irrefutável de ordem espontânea na prática.
> – Francis Pouliot

A Cripto-Cataláxia

A teoria praxeológica da cataláxia explica como a ordem *econômica* emerge de um sistema descentralizado, originado das ações descoordenadas e diversas de indivíduos que perseguem seus próprios interesses; é a ordem econômica espontânea. Às vezes chamado de "caláctica", o conceito econômico é um dos avanços intelectuais que permitiram aos defensores do livre mercado explicar como a sociedade evoluiu sem uma autoridade central. Hayek a define como "a ordem trazida pelo ajuste mútuo de muitas economias individuais em um mercado".

O termo obscuro capta a dinâmica que cria a civilização: a cooperação econômica espontânea entre indivíduos e grupos de indivíduos. Se os seres humanos devem se elevar acima do nível de Robinson Crusoé, eles devem interagir em benefício mútuo. A cooperação é tão valiosa para a liberdade individual que Satoshi forneceu o modelo da blockchain gratuitamente como uma forma de melhorar o mundo porque isso melhorou a vida dele. E fez isso segundo seu próprio interesse.

A revolução Satoshi exemplifica como o individualismo metodológico e a cataláxia trabalham juntos. O controle econômico é dado aos indivíduos. As pessoas armazenam suas riquezas em carteiras privadas, com as quais realizam comércio internacional sem passar por um sistema bancário, o que equivaleria a passar pelo estado. A descentralização é reforçada, e não contrariada, pela cooperação de uma rede de pessoas estranhas agindo, cada uma, em seu próprio interesse. E ainda assim, todos os estranhos se beneficiam, mesmo que não gostassem uns

dos outros casos se encontrassem pessoalmente. A criptoeconomia é a verdadeira sociedade econômica.

Ao longo da obra de Hayek, Mises e outros economistas pró-livre mercado, dois conceitos fundamentais emergem repetidamente: individualismo metodológico e ordem espontânea. Os dois conceitos são a espinha dorsal que forma a estrutura ideológica da cripto. Eles também explicam por que a explosão da cripto liberdade foi tão inesperada: surgiu dos indivíduos e da liberdade de ação, que estimulam explosões imprevisíveis de criatividade. Com as criptomoedas, a explosão ocorreu na área mais necessitada: a liberdade financeira.

A área mais difícil de implementar o individualismo metodológico é a financeira, porque ela foi controlada por muito tempo por um dos coletivos mais poderosos que existem: os bancos centrais, que funcionam como braços do estado. Isso significa que as instituições que cercam o banco central foram formadas por sua presença e por suas exigências, e que as atitudes financeiras comuns foram formadas de maneira semelhante.

A sociedade precisa ser lembrada: o estado não produz riqueza. No entanto, o estado precisa de grandes quantias para financiar a burocracia, os militares e outras armadilhas centralizadas do poder. Isso significa que o estado precisa roubar grandes quantidades de riqueza do setor privado – das pessoas comuns. Mas fazê-lo diretamente pode causar resistência na forma de revoltas fiscais ou em algo pior – pior para o estado, é claro. Assim, o estado emite títulos, moeda fiduciária compulsória, incentiva a inflação e compele todo o comércio a passar por instituições corporativistas – compadres dele – que estão sob seu controle. Muitas pessoas aceitam esse status quo como sendo “o jeito que o mundo gira”. Mas o que mais eles sabem? Outros, especialmente aqueles com compreensão da história, sabem que essa situação não é política ou moralmente inevitável, e muito menos necessária. No entanto, por muito tempo os rebeldes encontraram um caminho viável que fosse capaz de contornar a centralização das finanças.

Junte-se à cripto. É uma expressão pura do individualismo metodológico e da ordem espontânea. Mas “É” de que forma? As formas incluem:

- É a descentralização em larga escala. A engenharia central do dinheiro e seu fluxo é incorporada por leis de curso legal, dinheiro

fiduciário inflacionado, bancos centrais, leis de licenciamento financeiro, requisitos de relatórios e outros monopólios econômicos criados artificialmente pelo estado. Enquanto os indivíduos tiverem de seguir as regras do estado, especialmente o uso de fiat e bancos, não haverá liberdade financeira. No que pareceu um instante, mas que na verdade levou anos, Satoshi (e seus predecessores) descentralizou o dinheiro e seus meios de transmissão. As abstrações do estado e dos bancos centrais foram substituídas pelos indivíduos, que agem em seu próprio interesse.

- É descentralização consciente. O objetivo do Bitcoin e da blockchain é contornar a necessidade de uma terceira parte confiável, especificamente o banco central e o estado. A primeira linha de "Bitcoin: A Peer-to-Peer Electronic Cash System" diz: "Uma versão puramente peer-to-peer de dinheiro eletrônico permitiria que pagamentos online fossem enviados diretamente de uma parte para outra sem passar por uma instituição financeira". Ao fazer isso, a criptomoeda ignora as instituições usadas pela elite dominante para roubar riqueza.
- O dinheiro é valorizado pelos indivíduos. Os construtivistas acreditam que o dinheiro é uma construção social, que recebe significado e valor pelo estado da mesma maneira que os seres humanos recebem a humanidade por meio da socialização. Satoshi vira o mundo dos construtivistas de cabeça para baixo. O dinheiro do estado é uma fraude, e ele sabe disso. Os indivíduos que mineram e usam criptomoedas infundem valor nela sempre que a escolhem como meio de troca. E eles não apenas criam riqueza – os indivíduos também definem o valor dela.
- A cripto é profundamente individualista. Isso é verdade não apenas sobre suas funções, mas também sobre sua estrutura. Ela funciona através da involuntária cooperação de indivíduos auto interessados, como por exemplo os "mineradores". A estrutura da blockchain não pode ser centralizada ou nacionalizada; é descentralização exemplificada. Vladimir Putin de forma infame disse que "nem a Rússia, nem qualquer outro país, 'por definição', pode ter sua própria criptomoeda. Se falarmos sobre criptomoedas – isso é algo que vai além das fronteiras nacionais". As criptomoedas em uma blockchain chegam o mais próximo possível de uma

moeda que o estado não pode controlar ou centralizar. Alguns argumentam que as criptomoedas já são coletivistas, porque dependem de uma rede cooperativa de mineradores, nodes, desenvolvedores e administradores; alguns afirmam que a própria rede constitui uma terceira parte confiável. Mas isso não é verdade. A rede é um modelo de como um sistema independente de confiança opera na prática. A acusação confunde cooperação com coletivismo e consenso com planejamento central.

- A cripto expressa o mesmo tipo de ordem espontânea mundial que o conto "Eu, o Lápis." Em todo o mundo, estranhos involuntariamente cooperam uns com os outros para benefício mútuo. Suas valorações subjetivas e auto interessadas fortalecem algumas criptomoedas e desvalorizam outras, criando e atualizando uma taxa de câmbio para cada uma delas. As criptomoedas prosperaram precisamente porque é um imenso número de estranhos que controlam os nodes, que fazem as transferências, que inovam, que escrevem códigos e, no fim, cooperam. Cada ato é feito por motivos auto interessados, mas que acabam resultando em lucro para si e para os outros.
- A cripto pode parecer caótica, mas expressa uma ordem natural. A ordem centralizada lembra um desfile militar ou as obedientes filas indianas de triagem aeroportuária. A ordem espontânea assemelha-se a uma autoestrada movimentada onde os carros podem mudar de faixa constantemente, entrando e saindo à vontade. O que parece ser caos é uma forma sofisticada de organização, na qual estranhos voluntariamente participam. A autoestrada de aparência caótica leva as pessoas ao seu destino de desejo dia após dia.
- A cripto traz ordem ao campo monetário através de uma diversidade que oferece escolhas quase infinitas. Bancos centrais e instituições financeiras licenciadas pelo estado impõem a uniformidade, porque elas precisam que os clientes estejam em conformidade com os regulamentos e requisitos de relatórios do estado. A uniformidade imposta e a ordem centralizada não refletem as preferências dos indivíduos; eles refletem as preferências do estado. A comunidade cripto evita a uniformidade, porque a cripto atende a indivíduos cujas preferências são incrivelmente diversas. So-

mente quando "uniformidade" é usada como sinônimo de "ordem" que a cripto se torna *des*ordenada. Caso contrário, a cripto espelha o mesmo tipo de ordem que o pregão de uma bolsa de valores.

- O estado é irrelevante e é um obstáculo para a cripto. A centralização requer o estado ou algum substituto equivalente, porque a uniformidade não é natural e, para ser "aceita" deve ser empurrada goela abaixo. A descentralização, por sua vez, não requer um estado, porque não há conformidade forçada de ação ou preferência. Todas as escolhas são feitas livremente pelos indivíduos envolvidos.
- A cripto é a "mão invisível" da moeda. O termo descreve os benefícios sociais e econômicos não intencionais de ações tomadas pelos indivíduos visando seus próprios interesses. Ao perseguir seus próprios interesses financeiros, os usuários de cripto fazem muito mais para valorizar a moeda e criar práticas financeiras sólidas do que reformadores, que protestam por mudanças dentro do status quo sem questionar seus fundamentos… e sem conseguir resultados.

A cripto é uma expressão pura da economia austríaca.

Os Aspectos Revolucionários Não Reconhecidos da Cripto

A cripto lembra a "teoria do atirador solitário". Embora o termo seja geralmente associado ao assassinato do presidente John Kennedy e à subsequente Warren Commission, seu significado pode ser expandido. A história tropeça ao longo de um caminho bastante estável, embora nem sempre fácil, que é amplamente planejado pelo estado. Então um atirador solitário salta dos arbustos e atira no arquiduque Francisco Ferdinando, da Áustria, no Presidente McKinley, ou em JFK. A sociedade vira de cabeça para baixo. No caso de Ferdinando, o assassinato desencadeou a Primeira Guerra Mundial. A história muda para sempre, e a mudança não pode ser desfeita.

O controle estatal do mundo financeiro avançou esplendidamente ao longo do século XX – ou miseravelmente, dependendo da sua perspectiva. Uma rede mundial de controle foi lançada sobre as finanças dos indivíduos através de medidas como a Foreign Account Tax Com-

pliance Act (FATCA), que tentou garantir que os indivíduos que buscavam a liberdade não tivessem para onde ir com seu dinheiro. Então a cripto salta dos arbustos e assassina o sistema bancário. A história econômica muda para sempre, e a mudança não pode ser desfeita.

O efeito da cripto nas instituições financeiras estatais é bem conhecido, mas os efeitos sobre política social são menos discutidos. Previsivelmente, a explosão de liberdade que abalou o sistema bancário central também impactou outras instituições e políticas do estado. Aqui estão algumas poucas:

Política estrangeira. A comida é frequentemente usada como arma de política externa. Um artigo do *Free Thought Project* descreve como a blockchain neutraliza o uso belicoso de alimentos: "A tecnologia revolucionária da blockchain está ajudando a vítimas de desastres & alimentando os famintos sem estado". "Enquanto estados e banqueiros afirmam que criptomoedas e blockchain são ferramentas de criminosos, milhões de dólares em ajuda – gerados por essas tecnologias – estão ajudando os menos afortunados em todo o mundo". A ideia central do artigo é que as criptomoedas permitem que nações e indivíduos carentes contornem sanções econômicas impostas a eles por nações mais poderosas. Tornou-se mais difícil deixar as pessoas famintas por vantagens políticas.

Política doméstica. Quando o estado da Venezuela desvalorizou o Bolívar, removendo três zeros da moeda, os cidadãos migraram para a alternativa de livre mercado do bitcoin, com a qual eles já estavam familiarizados. "Nas economias avançadas, criptomoedas ativas como o bitcoin até agora tiveram pouco propósito além de especulação e jogos de azar. Mas nos países onde o sistema monetário e as estruturas financeiras estão desmoronando, o bitcoin pôde fornecer uma reserva alternativa de valor em relação à já demasiadamente inflacionada moeda local". A cripto resgata empresas; ela salva vidas.

O Controle Social do "Vício". A "Operação Chokepoint" foi uma operação bancária e política da era Obama, que atacava negócios supostamente indesejáveis, mas legais, como a venda de maconha medicinal, sexo e armas. O sistema bancário fechou contas, cancelou cartões de crédito e negou todos os seus serviços aos clientes "malfeitores". Essa prática está sendo revivida hoje. Mais uma vez, os bancos estão mirando nas lojas de maconha, nos profissionais do sexo e nas empresas de armas, independentemente de eles estarem ou não realizando um ne-

gócio legal. Cada vez mais, os vendedores de bens e serviços desaprovados têm adotado as criptomoedas como forma de sustentar seus meios de subsistência.

Proteção da Liberdade de Expressão. Depois de fazer circular documentos que constrangiam estados, o Wikileaks enfrentou um bloqueio bancário que acabou com as doações, que eram seu sangue vital. Então a Wikileaks abriu doações via bitcoin e a riqueza foi mais uma vez derramada sobre a empresa. A censura foi evitada. O mesmo acontece com a indústria pornográfica, que é um alvo da Operação Chokepoint.

O Livre Fluxo de Informações. Os processos contra a propriedade intelectual são geralmente baseados em seguir a trilha do dinheiro e descobrir os indivíduos do outro lado. Mas com o anonimato criptográfico, essa estratégia cai por água abaixo. Um artigo do site bitcoin.com, intitulado "Escritório de Propriedade Intelectual [IP] da UE: Bitcoin impede esforços antipiratataria", explica: "A ameaça inerente ao Bitcoin, de acordo com o relatório, é que as transações não podem ser facilmente vinculadas a um indivíduo no mundo real. Este problema é ruim para o EUIPO, uma vez que a aplicação dos direitos de autor é normalmente baseada na estratégia de seguir a trilha do dinheiro". Isso beneficia o fluxo global de informações.

Política de imigração. A imigração e a migração temporária são muitas vezes motivadas por um desejo de enviar dinheiro de volta para casa. Mas os migrantes também são frequentemente "desbancarizados" por instituições financeiras que exigem documentação, e a única alternativa é pagar taxas enormes para enviar dinheiro através de uma empresa privada, com suas famílias esperando dias pelas transferências. O presidente Trump ameaçou cortar esse incentivo à migração ao fechar ainda mais canais de transmissão. Mas, infelizmente, transferências rápidas e baratas via criptomoedas são incrivelmente difíceis de controlar.

O Estrangulamento dos Advogados e dos Tribunais. Contratos inteligentes são contratos jurídicos vinculados que usam software para auto executar os termos do contrato. Os contratos inteligentes peer-to-peer podem um dia se tornar onipresentes, desde negócios imobiliários até pedidos de seguro, o que reduzirá drasticamente a necessidade de advogados.

A Autonomia da Família. Os impostos sobre herança são hediondos porque são uma dupla tributação: assim que morre e passa suas pro-

priedades remanescentes para sua família, a pessoa cuja riqueza foi tributada por toda a vida é cobrada mais uma vez pelo estado. A cripto divide invisivelmente os bens entre os entes queridos – não há espaço para o estado na família.

Tudo isso é apenas uma pequena amostra do impacto revolucionário do uso das criptomoedas. As instituições que servem ao livre mercado estão sendo lentamente devolvidas ao controle e serviço dos indivíduos. As instituições que atendem ao estado estão sendo ignoradas e afundando cada vez mais.

As criptomoedas são o dinheiro da sociedade, não do estado. Sua evolução oferece um raro vislumbre de como instituições essenciais podem surgir em um livre mercado, sem a assistência do estado. A cripto de livre mercado é a manifestação do individualismo metodológico e da ordem espontânea em grande escala em uma área essencial da vida: a privacidade financeira.

Descentralização como Desobediência

A descentralização como estratégia para a liberdade acontece quando indivíduos buscam empoderar-se, separando-se do estado e reivindicando sua autonomia como indivíduos. Uma maneira de se separar é desobedecer à lei. A maioria das pessoas desobedece a lei de maneiras triviais e pacíficas todos os dias de suas vidas. Elas ignoram os limites de velocidade, constroem um anexo não autorizado à sua casa, cruzam o sinal vermelho, mentem nos formulários do estado, recebem pagamentos por baixo da mesa, queimam lixo no quintal, andam no meio da rua, recusam perguntas do censo, passeiam com o cachorro sem coleira ou sem licença e enviam mensagens de texto enquanto dirigem. Essas pequenas ofensas trazem pouco risco além de uma multa, mas mostram que as pessoas não se importam com a desobediência a leis que não fazem sentido ou que as incomodam de forma irracional.

Depois, há aqueles que desobedecem a lei de maneira mais séria. Eles sonegam impostos, estabelecem negócios não licenciados, usam drogas ilegais, mentem para a polícia, trocam sexo por dinheiro ou contrabandeiam. Esses delitos acarretam uma possível pena de prisão, mas a disposição das pessoas em desobedecer mostra que uma parcela significativa da população despreza as leis de crimes sem vítimas com tanto desprezo que elas as não cumprem, mesmo com risco considerável para seu bem-estar.

Nos anos 80, uma estratégia popular pela qual os indivíduos descentralizavam completamente suas vidas ficou conhecida como “Browning-out”, porque os praticantes usavam o livro best-seller de Harry Browne, *How I Found Freedom in an Unfree World: A Handbook for Personal Freedom,* como um modelo. Browne define a liberdade como viver a vida como você deseja viver enquanto permite que outros façam o mesmo. Em vez de protestar contra o estado ou buscar reformas distantes por meio de organizações, como os republicanos ou os democratas, Browne afirma que as pessoas podem desfrutar de um alto grau de liberdade aqui e agora. O capítulo 7 de seu livro, intitulado “As Armadilhas do estado”, afirma: “Mas quem é a ‘sociedade’, senão as pessoas que já expressam suas necessidades e preferências no mercado? Se elas não estão dispostas a pagar pelo serviço no livre mercado, quem pode dizer que estão dispostos a pagar por ele através do estado? Todas as ações do estado dependem de transações unilaterais, nas quais um indivíduo é forçado a escolher entre pagar pelo que não quer ou ir para a cadeia”. Aqueles que Browned-out (saíram como Browne) da Armadilha do estado descentralizaram o poder em suas vidas para o nível pessoal, onde eles eram a única autoridade sobre suas próprias escolhas.

Sair da sociedade tem um custo alto, no entanto. Não é apenas que o Estado tenta dar exemplos de dissidentes. É também que a sociedade é um benefício incrível para a humanidade. Facilita “bens” como conhecimento, prosperidade, cultura, progresso e autorrealização emocional de uma maneira impossível para os seres humanos isolados. Retirar-se torna-se preferível apenas quando uma sociedade é tão totalitária que constitui um perigo ou tormento para a própria vida. Esse é o ponto ao qual os escravos americanos arriscaram suas vidas para fugir do Norte, com cães e homens armados em seus calcanhares. Esse é o ponto ao qual pessoas desesperadas escalaram um muro de arame farpado em Berlim Oriental, apesar das armas apontadas em suas costas. Pessoas desesperadas tentaram escapar de uma selvageria que se faz passar por ordem social, e arriscaram suas vidas para fazê-lo.

A lição: a sociedade só tem valor para os indivíduos na medida em que eles têm a capacidade de dizer “não”. Nada é um “bem” incondicional; até mesmo o alimento com o qual a vida se sustenta não é um bem incondicional. Pergunte às pessoas que desejam cometer suicídio ou a um prisioneiro em greve de fome. O que é bom ou ruim depende de circunstâncias que devem ser avaliadas pelo próprio indivíduo. O

valor da sociedade depende da descentralização do poder, porque só assim os indivíduos que a compõem poderão sempre dizer "não".

A cripto fornece uma nova estratégia de liberdade, que evita muitas das desvantagens da desobediência aberta ou emigração; ela oferece uma revolução pacífica baseada no interesse próprio e que contorna o estado, em vez de enfrentá-lo. As pessoas podem dizer "não" a aspectos intoleráveis da sociedade, como o monopólio monetário, enquanto permanecem fisicamente conectadas com o resto.

Para muitos, uma revolução pacífica soa como uma contradição em termos. A confusão envolve a questão da revolução, porque ela foi mal retratada na ciência política e mal representada na realidade. Ruas com barricadas, pessoas em fúria, carros em chamas, confrontos com militares, gás lacrimogêneo, vitrines quebradas de lojas saqueadas... isso não é revolução. A verdadeira mudança vem dos corações e mentes das pessoas quando elas abraçam uma nova ideia, uma nova visão. A verdadeira revolução não é raiva e desespero; é esperança e realização.

John Adams escreveu a Thomas Jefferson sobre a Revolução Americana. "O que queremos dizer com Revolução? Guerra? Isso não fazia parte da Revolução. Foi apenas um Efeito e Consequência disso. A Revolução estava na mente do povo, e isso foi efetuado, de 1760 a 1775, no decorrer de quinze anos antes que uma única gota de sangue sequer fosse derramada em Lexington." Adams explicou onde a Revolução Americana poderia ser encontrada. "Os registros de treze legislaturas [coloniais], os panfletos, jornais em todas as colônias devem ser consultados, durante esse período". Durante quinze anos antes do levante, oradores e escritores vinham educando incessantemente o público sobre seus direitos naturais e a common law (lei comum). Essa foi a verdadeira Revolução Americana.

Uma revolução social nada mais é do que uma mudança fundamental em uma sociedade que transfere o poder de um grupo ou classe para outro. A verdadeira revolução ocorre somente depois que as bases intelectuais foram estabelecidas para mudar os corações e mentes de uma parcela suficientemente significativa da população; alguns estimam que a porção não deve ser superior a 10%. Se as bases intelectuais não foram estabelecidas, então as erupções violentas inevitavelmente se transformam em golpes, com um novo grupo de elites substituindo o antigo grupo. Enquanto for politicamente liderada, a revolução retornará ao "novo chefe, igual ao antigo chefe", e os indivíduos não serão empoderados.

Uma revolução de e para as pessoas comuns significa que a mudança no poder é descentralizada das elites para o nível individual. A violência apenas interfere nesse processo. É tentador especular o que teria acontecido se a revolução intelectual nas colônias americanas não tivesse sido interrompida pela violência. A verdadeira revolução referenciada por Adams estava lentamente conquistando a lealdade das pessoas comuns, e poderia ter produzido uma derrubada não violenta do jugo britânico. Como seria a América agora se não tivesse nascido com sangue? Felizmente, seu verdadeiro nascimento foi no papel de jornal, o que pode explicar por que terminou melhor do que a Revolução Francesa.

A explosão silenciosa causada por Satoshi em 2008 foi "uma revolução" porque derrubou a realidade do controle financeiro estatal e descentralizou o poder do estado para a pessoa comum. Aqueles que chamam o Bitcoin de revolucionário, no entanto, são descartados como hiperbólicos, porque a erupção criptográfica não está de acordo com as imagens de ruas ocupadas com barricadas e pessoas gritando "estado de merda!". Os pioneiros das criptomoedas não se assemelham a revolucionários armados, atirando na selva aos moldes de Che Guevara. O próprio Satoshi permanece anônimo, e isso é inédito para um líder revolucionário. E o Bitcoin rompe com esse estereótipo de revolução de várias maneiras. Foi uma revolução modesta e despretensiosa, em que nenhum sangue foi derramado. A área da vida que causou turbulência foi a finança – também conhecida como "lucro imundo" – e *isso* raramente é considerado uma causa nobre, digna de uma revolução. Não deveria uma bandeira que se preze dizer "LIBERDADE, JUSTIÇA" em vez de "DINHEIRO PRIVADO"?

Isso acontece porque a independência financeira é liberdade e justiça. A capacidade das pessoas de fazer e manter a riqueza que ganham é a maneira como elas alimentam seus filhos e perseguem sonhos; é como elas passam da fome ao bem-estar; a riqueza permite que as pessoas possuam a terra em que andam; o "lucro imundo" transforma uma assembleia de estranhos em uma sociedade civil, em indivíduos que negociam uns com os outros em vez de fazerem guerra uns contra os outros. O dinheiro é o motor da própria civilização porque a liberdade de expressão, a arte, a literatura e as outras incríveis conquistas humanas só acontecem quando as pessoas conseguem se alimentar.

A Revolução Satoshi é uma revolução das esperanças crescentes, que se tornou possível através da descentralização do controle econômico que as criptomoedas forjaram. É uma revolução de pessoas comuns, que agora têm uma alternativa viável ao fiat opressivo e aos bancos centrais.

"A revolução das esperanças crescentes" refere-se a uma situação em que mesmo um leve aumento na prosperidade e na liberdade leva as pessoas comuns a acreditar que podem melhorar suas vidas por meio de seus próprios esforços. Essa crença os faz exigirem mudanças políticas e econômicas que tragam mais liberdade e mais prosperidade. A pessoa comum não é uma lutadora da liberdade, e sua demanda por mudança não depende de ideologia. Depende do interesse próprio. Elas querem uma vida melhor para si mesmas e para seus filhos. E para *isso*, estão dispostas a lutar – principalmente de forma não violenta.

A frase "revolução das expectativas crescentes" surgiu depois que a Segunda Guerra Mundial desestabilizou a estrutura de poder do mundo. As ex-colônias do Extremo Oriente à América Latina e África se livraram do imperialismo e do despotismo, porque as pessoas comuns vislumbraram a possibilidade de finalmente alcançar mais liberdade e prosperidade.

O advento das criptomoedas desestabilizou a estrutura de poder financeiro do mundo e está causando uma segunda revolução de esperanças crescentes. Isso não ocorre em nível nacional – a cripto não reconhece fronteiras – mas sim na vida dos indivíduos, que podem finalmente controlar suas próprias finanças em privacidade e independentemente de permissão. Isso tem implicações políticas profundas, é claro, porque as pessoas independentes são muito menos propensas a obedecer.

Toda revolução bem-sucedida deve responder: "Qual é o ponto final?" Se não houver uma boa resposta, então um sistema ruim será substituído por outro sistema ruim, que despencará no vazio. A Revolução Francesa derrubou uma monarquia corrupta apenas para vê-la substituída por um "Comitê de Segurança Pública", que instituiu o que ficou conhecido como "O Reino do Terror". A revolução Satoshi deve responder: "Qual é o ponto final?". Gandhi disse: "os meios são os fins em andamento". Para aqueles que acreditam na cripto, a descentralização é o meio; a descentralização é o fim em andamento: o empoderamento total dos indivíduos.

Anarquismo: o Ponto Final da Descentralização

O homem nasce livre, mas encontra suas correntes em todo canto.
– Jean Jacques Rousseau

Existe tanta confusão e calúnia cercando o termo “anarquismo” que é útil, senão necessário, introduzir o conceito através de uma explicação… Daquilo que ele não é.

- Anarquismo não é violência. A maioria das tradições é explicitamente pacífica. O anarquismo não violento de Henry David Thoreau e de Mahatma Gandhi são exemplos.
- O anarquismo não é caos. Significa “sem estado”, e não “sem ordem”.
- Anarquismo não é pacifismo. Algumas formas, como o anarquismo cristão promovido por Leon Tolstói, mantêm o pacifismo como um princípio central, mas a maioria das tradições reconhece plenamente o direito de usar a força em autodefesa.
- O anarquismo não é inerentemente de esquerda. O anarquismo de esquerda recebeu a maior parte da atenção histórica, mas o primeiro anarquista americano foi o libertário Josiah Warren (1798-1874).
- O anarquismo não é um ideal impraticável. É uma abordagem realista para viver em sociedade sem sacrificar a individualidade.

Se isso tudo é aquilo que o anarquismo não é, então o que é o anarquismo? Simplificando, anarquismo significa “sem o estado”.

Mas o que é o estado? É a instituição que reivindica jurisdição sobre determinado território e o monopólio do uso da força. O estado é uma força institucionalizada, que exige obediência das pessoas que vivem neste território. O anarquismo olha para o estado e não vê serviços pelos quais as pessoas pagam impostos. Aquilo que é dito como serviço é, na realidade, monopólio sustentado pelo roubo e pela força.

Uma das maneiras mais fáceis de entender como o anarquismo funciona é perceber que é assim que a maioria das pessoas conduz suas vidas diárias. Elas vivem sem o estado, e nem se dão conta disso. O

anarquismo é a filosofia que eles seguem com a família, amigos, parceiros de negócios e até estranhos. Quando uma pessoa acorda de manhã, nenhuma lei a obriga a alimentar seus filhos com café da manhã em vez de deixá-los morrer de fome, ou a beijar sua parceira em vez de espancá-la. Quando ela pega carona com colegas para o trabalho, não há nenhum policial presente para impedi-lo de roubar seus bolsos ou socá-los no nariz. Ao longo do dia, nenhum burocrata fica por perto para garantir que ele pague por uma xícara de café ou contribua com sua parte da conta do almoço. Enquanto anda pela rua, um homem não ataca estranhos aleatórios ou puxa uma mulher para o beco a fim de molestá-la. Quando um estranho começa a sair do meio-fio em direção a um veículo que se aproxima numa velocidade considerável, alguém estende a mão rapidamente para impedir a pessoa.

Não é o estado que faz as pessoas agirem com decência habitual. É a sociedade civil, a família e os laços da humanidade que o fazem. A sociedade civil é naturalmente pacífica porque consiste em trocas voluntárias e não coercitivas. É da sociedade civil que os homens adquirem os hábitos e as recompensas da cooperação. Dito de outra forma, a maioria dos indivíduos já lida uns com os outros em suas vidas diárias como se todos vivessem sob a anarquia.

É o estado e outros criminosos que introduzem a força na vida cotidiana. O estado chega na forma da lei monopolizada através da ponta de uma arma. O estado diz a uma pessoa: “você não pode abrir um negócio, porque competiria conosco ou com alguma corporação favorecida por nós”. Diz que “sua propriedade não é sua para usar, mas nossa para administrar, tributar e confiscar se você se recusar a obedecer”. O estado rouba os ganhos de uma pessoa para sustentar seus próprios empreendimentos, até mesmo aqueles que causam repulsa na pessoa, como a guerra; o estado diz: “seu dinheiro é nosso para gastar como *nós* quisermos, e sua consciência não importa”. O estado exige a sua obediência a uma miríade de leis babás que trivializam o suposto direito de escolha individual que ele oferece. O estado tenta determinar até o tipo de canudo que alguém pode usar para beber refrigerante. O estado afirma: “você é meu para comandar.”

Em contraste, os anarquistas dizem às pessoas pacíficas: “abra qualquer negócio que desejar”; “sua propriedade é sua”; “seu dinheiro e sua alma são seus”, e “o estado não tem autoridade sobre você.”

Se o anterior não soa como o anarquismo que geralmente se discute, é porque existem diferentes tradições de anarquismo, e as mais

barulhentas e violentas recebem mais atenção. As várias formas de anarquismo incluem anarquismo individualista, anarquismo comunista, anarquismo socialista, anarquismo mutualista, anarquismo cristão, anarco-sindicalismo e anarcocapitalismo. O que os une? O que os separa?

As tradições dentro do anarquismo concordam que o estado é um tipo de grupo baseado na violência organizada e que é indesejável; é isso que une os anarquismos hifenizados – a rejeição do estado e da violência organizada como um todo. Onde eles discordam, porém, é sobre o que constitui violência e como uma sociedade sem ela funcionaria.

Eis o contraste entre as abordagens dos anarquismos comunistas e individualistas.

O comunismo vê o capitalismo laissez-faire como uma forma de roubo, que é uma forma de violência. Um dos motivos é o "valor excedente" – a famosa mais-valia. Popularizado por Karl Marx, esse conceito refere-se ao valor supostamente criado pelos trabalhadores, que excede os custos de seu trabalho e produção. De forma simplista: Um operário ganha $1 por hora e usa matéria-prima que custa $1 para produzir um bem que é vendido por $10. Segundo Marx, uma mais-valia de $8 foi criada pelo trabalhador, que é o legítimo proprietário dessa quantia. A mais-valia é embolsada pelo dono da fábrica capitalista em um ato de roubo. O capitalista é capaz de roubar os $8 porque possui os meios de produção que são protegidos pela força do estado. Assim, o capitalismo está irrevogavelmente enredado na exploração dos trabalhadores e na violação de seus direitos. Para os esquerdistas, o anarquismo é necessariamente antiestatista e anticapitalista porque ambos são formas de violência.

O anarquismo individualista desafia essa interpretação. Ele olha para o mesmo operário e proprietário da fábrica e vê uma relação consensual pela qual o trabalhador recebe um salário com o qual ambos concordaram e através do qual ambos se beneficiam. A chamada mais-valia ou lucro que o capitalista recebe é em troca dos riscos de fazer negócios, das despesas gerais, do investimento contínuo de capital, dos custos de propaganda e do custo de seu próprio tempo. Nenhuma força ou fraude está presente. Desde que o estado não promova o lucro do capitalista, fazendo nada além de fazer valer os direitos de propriedade – por exemplo, ele não lhe concede um monopólio – então nenhuma força ou fraude está presente devida ao estado. A fábrica expressa apenas o livre mercado e a troca voluntária.

Se o estado intervém, aprovando leis que favorecem ou prejudicam os negócios, então o arranjo deixa de ser de livre mercado ou capitalismo de laissez-faire e se torna capitalismo de compadrio; este é um arranjo no qual o estado e algumas empresas se alinham em benefício mútuo e em desvantagem de todos os outros. Os que mais sofrem são os trabalhadores, as empresas concorrentes e os consumidores. Para os anarquistas individualistas, o anarquismo é antiestado e anti-comparsas-do-estado. O anarquismo individualista é pró-mercado e capitalista.

O profundo desacordo sobre o livre mercado tem implicações para os conceitos-chave usados por ambas as formas de anarquismo. Por exemplo, o anarquismo comunista e o anarquismo individualista definem “classe” e afiliação de classe de maneiras drasticamente diferentes. O anarquismo comunista define a filiação de classe de uma pessoa por referência à sua relação com os meios de produção; alguém é trabalhador ou capitalista; ele é explorado ou explorador. As duas classes estão presas em uma guerra de classes sem fim.

Em contraste, o anarquismo individualista define a filiação de classe com referência à relação de uma pessoa com o poder do estado; ele coopera com os outros de forma voluntária (sociedade) ou usa a força (o estado). Ou ele é um membro produtivo da sociedade ou ele é um criminoso. Os anarquistas individualistas veem as duas classes – a sociedade e o estado – presas em uma guerra de classes insolúvel.

Em resumo: embora todas as formas de anarquismo rejeitem o estado e sua violência organizada, algumas formas de anarquismo discordam profundamente sobre o que constitui violência.

O que é o Anarquismo Individualista ou Libertário?

> Isso nos leva ao Anarquismo, que pode ser descrito como a doutrina de que todos os assuntos dos homens devem ser administrados por indivíduos ou associações voluntárias, e que o estado deve ser abolido. Quando Warren e Proudhon, prosseguindo em sua busca por justiça ao trabalho, se depararam com o obstáculo dos monopólios de classe, viram que esses monopólios repousavam sobre a Autoridade, e concluíram que a coisa a ser feita era não fortalecer essa Autoridade e assim tornar o monopólio universal, erradicar totalmente a Autoridade e dar total domínio ao princípio

oposto, a Liberdade, tornando a competição, a antítese do monopólio, universal.
– Benjamin R. Tucker

Aqueles que chamam a si mesmos de individualistas ou anarquistas-libertários não concordam em todos os aspectos da teoria. Afinal, eles são anarquistas. O que precede, entretanto, é a visão dominante. O anarquismo individualista geralmente se baseia na Lei Natural da qual surgem os direitos naturais ou individuais. A palavra “Lei” aqui não é usada em sentido legal ou legislativo. Refere-se a um princípio ou uma regra governante, como as leis da física. “Natural” significa que a lei é baseada nos fatos da realidade e na natureza do homem.

Em sua forma mais simples, a versão da Lei Natural usada pelo anarquismo individualista é uma tentativa de fundamentar os valores humanos nos fatos da realidade e da natureza humana. Dito de outra forma: Dado o que sabemos sobre a realidade e sobre a natureza humana, é possível raciocinar regras de comportamento que maximizem o bem-estar dos seres humanos? O anarquismo individualista responde “sim!” e se volta para o conceito de direitos naturais ou individuais. Ele pergunta: “quem é o dono do indivíduo?” Como discutido anteriormente, existem apenas três respostas possíveis: é o indivíduo (liberdade pessoal), é alguém ou alguma outra coisa (escravidão), ou ele é propriedade não reclamada. O anarquismo individualista argumenta fortemente a favor da primeira posição.

A reivindicação de uma pessoa sobre seu próprio corpo é descrita com diferentes termos, incluindo “soberania do indivíduo”, “donidade de si mesmo”, “autonomia”, “autopropriedade” e “direitos individuais”. Mas para reivindicar seu direito inato de liberdade, todo homem deve respeitar a liberdade igual dos outros. Se ele inicia a força, então suas ações constituem uma declaração de que ele não considera a liberdade como seu direito de nascença ou qualquer direito. Os direitos são universais – existem no mesmo grau dentro de cada ser humano – ou não são baseados na natureza humana. É este dever de respeitar os direitos dos outros que um indivíduo carrega consigo dentro da sociedade.

Direitos e deveres são as ferramentas pelas quais a sociedade resolve conflitos e evita a violência. O individualista do século XIX Benjamin R. Tucker usa essa abordagem enquanto especula sobre a natureza da propriedade. Tucker acredita que as ideias surgiram apenas porque atendem a uma necessidade ou porque respondem a uma pergunta.

Para ilustrar seu ponto de vista, Tucker pede aos leitores que imaginem um universo paralelo ao nosso, mas que siga regras diferentes. Nesse universo paralelo, os habitantes podem satisfazer suas necessidades simplesmente desejando bens. Comida aparece magicamente em suas mãos, roupas milagrosamente cobrem seus membros e uma cama surge sob seus corpos cansados. É pouco provável que essa sociedade paralela venha com o conceito de propriedade privada. Por quê?

Tucker pergunta: “O que há na realidade de nosso próprio mundo e na natureza do homem que dá origem ao conceito de propriedade em primeiro lugar?”. Ele conclui que a ideia de propriedade surge como forma de resolver conflitos causados pela escassez. No universo real, quase todos os bens são escassos, e isso leva à competição pelo seu uso. Como a mesma cadeira não pode ser usada da mesma maneira ao mesmo tempo por duas pessoas, é necessário determinar quem deve usar a cadeira. O conceito de propriedade resolve esse problema social. O proprietário da cadeira deve determinar seu uso. “Se fosse possível”, escreve Tucker, “e se sempre tivesse sido possível, para um número ilimitado de indivíduos usar em uma extensão ilimitada e em um número ilimitado de lugares a mesma coisa concreta ao mesmo tempo, jamais teria sido instituída qualquer coisa como a propriedade.”

Quaisquer direitos, deveres e propriedades são derivados – seja da lei natural ou do utilitarismo. Eles são o contexto que os indivíduos trazem consigo quando entram na sociedade.

Uma Saudação a Henry David Thoreau

Poucos filósofos do século XIX usaram a sua própria capacitação com tanta graça quanto o americano Henry David Thoreau. Ele tinha boas razões para se perguntar: “Como o indivíduo lida com um estado moralmente intrusivo?” Sua solução é simples; jogue o estado fora de sua vida e nunca olhe para trás. Foi isso que Thoreau fez na vida real.

O tratado político mais famoso de Thoreau se chama *Desobediência Civil*. Foi sua resposta a uma prisão durante a noite de 1846 por se recusar a pagar um imposto que violou sua consciência. Uma troca famosa e talvez anedótica ocorreu enquanto ele estava preso. Ralph Waldo Emerson o visitou e cobrou-lhe o pagamento de uma multa para que fosse libertado.

Emerson pergunta: “Henry, o que você está fazendo aí dentro?”

Thoreau responde: "Waldo, a verdadeira questão é: o que você está fazendo aí fora?"

Thoreau não ficou amargurado com sua breve prisão. Perto do fim de sua vida, ele foi perguntado: "Você fez as pazes com Deus?" Ele respondeu: "Nunca briguei com ele". Para Thoreau, esse teria sido o custo real do pagamento do imposto; significaria brigar com sua própria consciência, o que seria semelhante a brigar com Deus.

A Desobediência Civil termina com uma nota feliz. Após a libertação de Thoreau da prisão, as crianças de sua cidade natal imploraram para que ele se juntasse a uma caçada por mirtilos. Caçar mirtilos era um dos passatempos valiosos de Thoreau, e sua habilidade em localizar arbustos carregados de frutas o tornou o favorito das crianças. Ele termina sua crônica de prisão com as palavras: "Eu me juntei a um grupo de caçadores de mirtilos, que estavam impacientes para se submeterem à minha liderança; e em meia hora estávamos no meio de um campo de mirtilos, em uma de nossas colinas mais altas, a duas milhas de distância, e lá o estado não foi visto em lugar algum."

E lá o estado não foi visto em lugar algum. Este é o legado de Thoreau e Satoshi para aqueles que desejam compreender isso: para aqueles que estão dispostos a abandoná-lo e não olhar para trás, o estado não será visto em lugar algum. Thoreau, em sua alegria de correr com as crianças, sabia que a prisão não era a sua realidade. Caçar mirtilos era a sua realidade.

O que resta quando não há estado? Indivíduos, sociedade… e mirtilos![1]

1 Nota de Tradução: Um trecho dessa parte específica foi uma adição considerada pertinente pela equipe de tradução. No original lê-se Individuals and Society (indivíduos e sociedade).

SEÇÃO QUATRO

Estado e Sociedade

Relevância do Estado, da Sociedade e da Obediência para a Cripto

> O muro que separa o estado e a sociedade está desmoronando. Ou melhor, o estado está martelando em uma tentativa agressiva de controlar todos os aspectos da vida produtiva e cooperativa. […] As pessoas com quem você lida diariamente estão deixando de ser bons vizinhos, comerciantes honestos e estranhos desinteressados. Eles estão se tornando informantes do estado que monitoram sua expressão, seu dinheiro, seu comportamento e atitude para denunciá-lo às autoridades. Eles estão deixando de ser "sociedade" e se tornando "o estado".
> – Murray Rothbard, "Society Without State".

O liberalismo clássico traça uma distinção nítida entre o estado e a sociedade, que as criptos adotam. A cripto não foi projetada para imitar moeda emitida pelo estado ou sistemas monetários controlados pelo estado. Sua estrutura e função foram criadas para empoderar o indivíduo através do fornecimento de meios livres do estado para alcançar a independência financeira. Seus fins e seus meios são tão compatíveis com a sociedade quanto antagônicos ao estado.

Os conceitos e realidades de estado, sociedade e obediência são o contexto no qual o Bitcoin nasceu e no qual as criptomoedas agora operam. Para entender o passado, presente e futuro das criptomoedas, é necessário entender esses conceitos.

A Estrutura do estado, da Sociedade e das criptomoedas

> O problema dos meios é, a meu ver, um problema duplo: primeiro, o problema do fim e dos meios; segundo, o problema do Povo e do estado, ou seja, os meios pelos quais o povo pode supervisionar ou controlar o estado […]. Os meios devem ser proporcionados e adequados ao fim, pois são meios para o fim, por assim dizer, o próprio fim em seu próprio processo de vir à existência. De modo que aplicar

> meios intrinsecamente maus para alcançar um fim intrinsecamente bom é um simples absurdo e um fracasso. – Jacques Maritain, *Man and The State*.

Um método simples para entender a diferença entre o estado e a sociedade é analisar seus meios e fins.

O fim de um estado é regular a sociedade para manter sua existência e fazer valer seus privilégios. Seu privilégio primordial é o monopólio do exercício da violência sobre as pessoas e propriedades dentro de um território definido. O estado usa a força na forma de lei ou a ameaça da lei para impor suas políticas. Atrás de cada lei está uma arma com a possibilidade de irromper violência se a lei não for obedecida. No entanto, o estado prefere obter a complacência do que ter de punir alguém, porque a punição é um processo desajeitado que pode inspirar resistência. O estado prioriza a aquisição de riqueza porque não produz nada e não tem receita, exceto o que é derivado de outros por meio de ameaças ou violência. Em outras palavras, aqueles que estão no poder usam o monopólio da força como meio de criar e sustentar o privilégio desejado.

A sociedade é a interação voluntária dos indivíduos com as instituições que evoluem das associações. Uma instituição é um costume, padrão de comportamento ou relacionamento dentro da dinâmica de uma sociedade; casamento, igreja ou a família são exemplos. O dinheiro é uma instituição vital tanto para o estado quanto para a sociedade.

O objetivo da sociedade – se é que se pode dizer que uma rede altamente descentralizada tem um propósito consciente – é ser um local no qual os indivíduos possam trocar por benefício mútuo, seja esse benefício definido em termos econômicos, espirituais ou outros. A sociedade é voluntária, com obrigações legais decorrentes apenas de consentimento e contrato. Este é o meio social: a livre associação. O fim ou objetivo da sociedade é expresso por cada membro que age em seu próprio interesse. Como os indivíduos são diversos e imprevisíveis, a forma da sociedade é fluida e imprevisível, exceto por não ser violenta.

"A forma segue a função" significa que a forma básica de qualquer coisa é determinada pelo seu propósito. A forma de uma cadeira é ditada por sua função como estrutura sobre a qual as pessoas se sentam, e é por isso que uma cadeira de sucesso tem uma superfície estável. Para o arquiteto Frank Lloyd Wright, a forma e a função de uma coisa tinham que ser inseparáveis para que sua síntese fosse bem-sucedida. "A forma

segue a função – isso foi mal compreendido”, observa Wright. “Forma e função devem ser uma, unidas em uma união espiritual.” Se os dois estiverem em conflito, então a forma falha ou a função revela-se diferente do que foi declarado. Se manter a paz envolve matar pessoas inocentes, por exemplo, significa que manter a paz não é o fim a ser expresso. Durante a Guerra do Vietnã, um oficial do exército dos EUA justificou o bombardeio de áreas civis na província de Bến Tre, no delta do Mekong, com a declaração: “Tornou-se necessário destruir a cidade para salvá-la”. Essa explicação se transformou no infame ditado: “Tivemos que destruir a vila para salvá-la”. Uma forma e uma função discordantes muitas vezes revelam uma função oculta e verdadeira.

Mahatma Gandhi expressou famosamente a conexão entre forma e função na dinâmica social. “Se cuidarmos dos meios”, escreve ele, “o fim cuidará de si mesmo”. Isso refletia a realidade dos meios serem os fins em andamento. Gandhi não desvaloriza a importância do fim à vista, mas reconhece que cada estágio dos meios deve expressar o fim em uma progressão lógica para que o fim se materialize.

A maioria das pessoas se concentra em objetivos, como prosperidade, e depois descobre como alcançá-los. As estratégias são vistas como pragmáticas e quase intercambiáveis: o que funciona ou oferece um atalho. Mas a crueldade não pode levar a relacionamentos amorosos; só a benevolência pode. O roubo não cria respeito pelos direitos de propriedade; só a honestidade o faz. Se o objetivo das criptomoedas é libertar indivíduos financeiramente, então o meio de alcançá-lo é inseparável desse fim. Os meios são o respeito aos direitos individuais, aos livres mercados, à paz e à sociedade. As estratégias opostas são o coletivismo, os monopólios e a violência, sendo o estado um resultado previsível.

“Deveria haver uma lei” é uma solução instintiva comum para alcançar quase qualquer objetivo social nos dias de hoje; as pessoas clamam por usar a violência institucionalizada do estado, a fim de promulgar leis que punam ou incentivem outros a aceitar um fim desejado que não aceitariam de bom grado. O objetivo pode ser comparativamente modesto, como impor um código de vestimenta pelo qual homens, e não mulheres, ficam de topless. Ou pode ser abrangente como a imposição de uma determinada doutrina religiosa. A reação reflexiva de “deveria haver uma lei” ignora a questão de saber se os meios e os fins estão em conflito. Poucas pessoas perguntam se é mesmo possível que a lei imponha ideias e atitudes, pensamentos e sentimentos; não é. O

máximo que é possível é que a lei intimide as pessoas a expressar externamente pensamentos e sentimentos "corretos", apesar do que pensam e sentem por dentro.

Como tais leis interferem na liberdade de consciência e de expressão de um indivíduo, uma sociedade livre não as impõe; como meio, tais leis contradizem os fins da sociedade. No entanto, por conferirem ao estado imenso poder sobre sua população, tais leis são uma prática padrão para aqueles que estão no poder; como meio, eles atingem os fins desejados. Quanto mais vaga for a declaração de uma meta – "igualdade de renda" ou "justiça social" – mais poder ela confere ao estado, porque a definição é elástica. Com a cripto de livre mercado, o fim está bem definido: uma transferência descentralizada e privada de fundos ou outras informações em uma rede peer-to-peer. Com fiat e o sistema bancário, o fim é subjetivo e aberto à redefinição: estabilidade monetária.

Todo mundo sabe que alguns objetivos exigem meios específicos. Manter-se saudável requer comer bem, praticar exercícios e adotar bons hábitos. Os meios apropriados tornam-se menos óbvios quando o fim é complexo, amorfo ou não expresso com franqueza. De alguma forma, a conexão lógica entre os dois se perde. "Os fins justificam os meios" tornou-se uma desculpa para abandonar as considerações práticas e morais sobre como alcançar objetivos específicos. Uma vez que um fim é estabelecido, um menu de meios é examinado para aqueles que devem atingir o objetivo da forma mais rápida e econômica possível. Questões mais fundamentais sobre a relação entre meios e fins raramente são feitas. A guerra pode realmente trazer a paz? A censura pode criar uma sociedade aberta? A proibição de criptomoedas protege a segurança financeira?

Quando os fins e os meios entram em conflito, o fim torna-se uma impossibilidade prática. Uma pessoa que declara que "os fins justificam os meios" ou está muito equivocada sobre como os objetivos são alcançados, ou tem em mente um objetivo totalmente diferente do que é declarado. A utilização de um meio hostil para a obtenção de um fim introduz um elemento orwelliano. O duplipensar intrínseco no slogan da Primeira Guerra Mundial "Uma guerra para acabar com todas as guerras" é óbvio. Os meios obviamente falharam em atingir o objetivo declarado, porque a eliminação do conflito nunca foi o objetivo real; território, poder e lucro foram o propósito da Primeira Guerra Mundial. O falso objetivo foi aceito, no entanto, e ainda é alardeado, embora não

faça sentido. Ninguém fala de “Uma Verdade para Acabar com Todas as Verdades”, “Um Argumento Lógico para Acabar com Toda a Lógica” ou “Uma Virtude para Acabar com Todas as Virtudes” porque estes são absurdos autocontraditórios. A maneira de acabar com a guerra não é travá-la, mas recusar o engajamento. O meio – travar uma guerra – é diametralmente oposto ao fim declarado – prevenir mais guerra. Quando isso ocorre, é hora de olhar sob a superfície para a intenção real.

Isso revela uma profunda diferença ideológica entre os defensores do estado e os defensores da sociedade ou do livre mercado. Os estatistas são orientados para os fins; defensores da sociedade civil são orientados para os meios. Isso não sugere que a sociedade civil – isto é, os indivíduos dentro dela – não tenha ou estabeleça objetivos específicos. Diz que a sociedade percebe que os meios adequados para atingir qualquer fim devem ser empregados. Em contraste, os estatistas se concentram inteiramente no fim e usam todo e qualquer meio necessário ou conveniente para alcançá-lo.

Os estatistas fornecem um plano detalhado para o que constitui uma sociedade justa, por exemplo. Um fim declarado dessa sociedade pode ser uma igualdade socioeconômica, que exija que o estado monopolize todas as questões monetárias, incluindo o comércio, para garantir a distribuição adequada de riqueza e oportunidades. O fim dita os meios. Isso vale para uma sociedade moral, qualquer que seja a definição de “moralidade” empregada. O fim exige que o estado monitore o comportamento, as palavras e as atitudes expressas por cada indivíduo. Sempre que um fim específico é identificado como um objetivo primordial e independente, então o uso da força torna-se necessário para impô-lo a pessoas que discordam pacificamente, porque alguém sempre o fará.

Em contraste, a abordagem de livre mercado é orientada para os meios. Uma sociedade justa não visa um resultado como um arranjo socioeconômico específico. Quaisquer arranjos que resultem de indivíduos fazendo escolhas livres e pacíficas são considerados justos. O que quer que seja voluntário é justo – ou, pelo menos, tão próximo disso quanto os seres humanos imperfeitos em um mundo imperfeito podem chegar. Por exemplo, uma faculdade particular que discrimine negros e uma que aplique uma política somente para negros existiriam lado a lado no mercado. Desde que ambos sejam financiados por fundos privados e ninguém seja obrigado a participar, ambos os arranjos são justos

e a lei não pode interferir adequadamente. Se as pessoas consideram as políticas escolares imorais, elas são livres para usar uma ampla variedade de meios pacíficos para promover mudanças. Essas estratégias incluem educação, protesto, piquetes, boicote e persuasão moral. O que eles não podem fazer é usar a força para ditar a maneira como as faculdades usam seu próprio dinheiro para estabelecer suas próprias políticas. A liberdade de associação exige o direito de discriminar.

Os estatistas não são igualmente restritos. Sua primeira escolha ao buscar "reformar" uma prática pacífica, mas imoral, é aplicar a força institucional da lei.

O filósofo francês do século XX, Jacques Maritain, considerou o "o dilema dos meios versus os fins" como o problema da filosofia política. A Revolução Francesa forneceu a ele o modelo de como um fim falhou miseravelmente porque os meios usados para alcançá-lo eram "intrinsecamente maus". Em uma revolução estereotipada, os indivíduos se levantam em massa para tomar o poder da elite e dos governantes opressores. As revoluções são chamadas de "populares" porque começam com uma onda de resistência popular contra o status quo. E é verdade; é assim que muitas revoluções começam. E então elas se desenrolam de maneira terrivelmente errada. A França foi de uma monarquia absoluta, que devastou os direitos das pessoas comuns, à "uma pessoa superior chamada estado Nação", que devastou os direitos das pessoas comuns. A prometida "Liberté, Égalité, Fraternité" (Liberdade, Igualdade, Fraternidade) nunca se materializou. Em vez disso, autocratas sanguinários como Robespierre e Saint-Just, juntamente com uma nova classe de burocratas mesquinhos, realizaram prisões e execuções em massa que geralmente visavam pessoas comuns que violavam as leis econômicas – contrabando, por exemplo.

A Revolução Bolchevique é outra lição de moral. O catastrófico número de mortos e fome causados pelo envolvimento da Rússia na Primeira Guerra Mundial, mais do que um compromisso com o marxismo, levou os russos à revolta. As terceiras partes confiáveis chamadas "líderes" levaram a sociedade longe demais, e eles perderam toda a confiança. Seu colapso deixou um vazio de poder. Sob o lema "Paz, Pão e Terra", oficiais revolucionários correram para preencher esse vazio com um regime totalitário e dogmático, em vez do paraíso dos trabalhadores que eles mesmos haviam prometido. É o caminho desgastado das revoluções; conheça o novo chefe, igual ao antigo chefe.

Essas revoluções não atingiram "o objetivo final e a tarefa mais essencial do corpo político ou da sociedade política", explica Maritain. A tarefa era "melhorar as condições da própria vida humana" e "procurar o bem comum da multidão, de tal maneira que cada pessoa concreta, não apenas em uma classe privilegiada [...] pudesse verdadeiramente alcançar essa medida de independência que é própria à vida civilizada". Em termos coloquiais, Maritain está dizendo: "você não pode chegar lá a partir daqui".

Por quê? Porque os líderes revolucionários se tornaram um novo conjunto de terceiras partes confiáveis. Os revolucionários formaram uma nova elite, que adotou a mesma estrutura básica de poder de antes: governo absoluto que governa por meio de reivindicações de legitimidade, intimidação e força bruta. Mudaram-se os rostos, as ideologias e os fins declarados, mas não os meios de poder centralizado que se impunham pela força institucionalizada. Os revolucionários usaram os mesmos meios que seus predecessores, e chegaram aos mesmos resultados: a opressão das pessoas comuns. Somente se mudando os meios – apenas descentralizando o poder de volta para o indivíduo – uma revolução pode evitar se transformar em só mais um estado. Somente quando os líderes revolucionários deixarem de evoluir para uma terceira parte confiável, que um Robespierre, um Lenin, um Pinochet, um Mao ou um Castro deixarão de ser inevitáveis.

A revolução das criptomoedas resolve o Dilema Meios Versus Fins dentro da filosofia política, porque as criptomoedas são o meio e o fim ao mesmo tempo. Gandhi também afirma: "Não há muro de separação entre meios e fins. Meio e fim são termos sinônimos em minha filosofia de vida." Eis a estratégia das criptomoedas: descentralizar as trocas financeiras por meio de uma blockchain, a fim de contornar terceiras partes confiáveis e devolver o controle monetário ao indivíduo. O fim político: descentralizar as trocas financeiras para contornar terceiras partes confiáveis e devolver o controle monetário ao indivíduo. O meio e o fim são um no mesmo. O processo pseudônimo, descentralizado e peer-to-peer é transformador. Quando a flexão do poder individual se torna suficientemente difundida, torna-se uma revolução sem líder – uma revolução independente de confiança – que depende de indivíduos perseguindo seus próprios interesses. Os meios são "qualquer coisa que seja pacífica". O fim é o que resulta dos meios.

O estado Contra a Sociedade

Em sua obra clássica, *The State* (1914), o sociólogo alemão Franz Oppenheimer encabeça uma análise dos dois termos mais importantes na discussão política: “o estado” e “a sociedade”. Os termos antitéticos, cada qual expressa um modo de organização humana e cada um reflete a importância da riqueza ou produtividade para a existência humana. A condição natural do homem é a pobreza. Um bebê nasce com nada além de seu próprio desamparo, e morrerá sem a intervenção tenaz de um cuidador. Uma vez que uma pessoa é capaz de usar seu trabalho para transformar recursos ou criá-los, então ela é capaz de cuidar de si mesma através de um esforço contínuo. A produção de riqueza é literalmente o que permite que as pessoas sustentem suas vidas. A habilidade de produzir e controlar a riqueza é uma questão de vida ou morte.

Oppenheimer identifica dois meios antagônicos pelos quais a riqueza é controlada: o estado e a sociedade. Ele define o estado como “a soma de privilégios e posições dominantes que são criadas pelo poder extraeconômico”. As palavras “poder extraeconômico” significam força ou ameaça de força. As instituições do estado incluem os militares, a imposição da lei, as legislaturas e as burocracias. Seu denominador comum é a administração e manutenção do poder estatal através do uso da violência institucionalizada. “Eu defino o estado”, escreve Rothbard, “como aquela instituição que possui uma ou ambas (quase sempre ambas) das seguintes propriedades: (1) adquire sua renda pela coerção física, conhecida como ‘tributação’; e (2) afirma e geralmente obtém o monopólio coagido da prestação de serviços de defesa (polícia e tribunais) sobre uma determinada área territorial. Uma instituição que não possua nenhuma dessas propriedades não é e não pode ser, de acordo com minha definição, um estado”.

Oppenheimer define a sociedade como “a totalidade de conceitos de todas as relações e instituições puramente naturais entre homem e homem”. As palavras “puramente natural” significam “voluntário”, sendo a sociedade a soma total das interações pacíficas dos indivíduos dentro dela. As instituições da sociedade incluem o livre mercado, os locais de adoração, as escolas, as instituições de caridade e as artes. Rothbard descreve a sociedade como um lugar “onde não há possibilidade legal de agressão coercitiva contra a pessoa ou propriedade de um indivíduo”. Os anarquistas se opõem ao estado porque ele tem seu próprio ser em tal agressão, a saber, a expropriação da propriedade privada

por meio de impostos, a exclusão coercitiva de outros prestadores de serviços de defesa de seu território e todas as outras depredações e coerções que são construídas sobre esses focos gêmeos de invasões de direitos individuais”. O estado é chamado de esfera pública; a sociedade é a esfera privada.

(Nota: O estado e a sociedade são abstrações, e deve-se tomar cuidado para não torná-los em algo excessivamente concreto. A abordagem analítica do liberalismo clássico é o individualismo metodológico, que afirma que apenas os indivíduos existem e agem. Todas as instituições – incluindo as de ambos o estado e a sociedade – podem ser reduzidas às ações dos membros individuais de cada instituição).

A riqueza pode ser controlada pelo estado ou pela sociedade – isto é, pelos membros individuais de ambos – mas só pode ser produzida pela sociedade. O estado emprega o que Oppenheimer chama de “meio político” – isto é, força ou ameaça de força – para adquirir a riqueza que não produz nem adquire por meio de troca voluntária. A riqueza é retirada de pessoas que produzem e trocam, o que Oppenheimer chama de “meio econômico” de adquirir bens.

O estado não costuma tomar a riqueza pela força bruta, no entanto. Em vez disso, o estado usa métodos de roubo mais sutis e menos arriscados. Por exemplo, canaliza a produtividade da sociedade para uma forma de dinheiro que monopoliza ao emiti-lo e impõe leis de curso legal. Então, o monopólio monetário é consolidado regulando as instituições financeiras através das quais o dinheiro é forçado a fluir. Isso permite que o estado realize roubos sutis, como a inflação. A violência direta é o monopólio monetário, que proíbe e pune os concorrentes do livre mercado.

Expresso de outra forma: O fim do estado é manter sua existência e poder. Para cumprir esse objetivo, o estado precisa da riqueza e da cooperação da sociedade, pois não produz riqueza. O estado precisa roubar da sociedade porque sua única fonte de “renda” é o que ele obtém através de meios que incluem impostos, confiscos, multas, taxas, tarifas, inflação e subornos. A força e as ameaças de força são os meios necessários – os meios políticos –: os meios do estado.

Em contraste, a sociedade não tem fins. Embora seja um motor de criação e troca, a sociedade não tem consenso sobre quais devem ser os resultados dessa produtividade. Cada membro individual age para perseguir seu interesse próprio, com cada pessoa tendo uma definição única do que compreende esse objetivo. O objetivo de uma pessoa pode

ser ganhar um milhão de dólares, enquanto o de outra pode ser adquirir educação. O meio pelo qual cada indivíduo atinge seu objetivo é através da criação e do comércio – os meios econômicos – que produzem sua própria versão de riqueza. Novamente, o que constitui riqueza difere de pessoa para pessoa, e inclui dinheiro, cultura, conhecimento, família, espiritualidade e todos os outros valores humanos possíveis. Os meios da sociedade são o oposto da coerção, porque uma troca ocorre apenas quando todas as partes de uma transação concordam com seus termos e todas as partes se beneficiam.

Rothbard destaca a principal diferença entre interagir com a sociedade e com o estado.

> Se eu deixar ou me abster de comprar cereais no mercado, os produtores de cereais não virão atrás de mim com uma arma ou ameaça de prisão para me obrigar a comprar; se eu não conseguir entrar na American Philosophical Association, a associação não pode me forçar a entrar ou me impedir de desistir de minha filiação. Somente o estado pode fazê-lo; só o estado pode confiscar minha propriedade ou me colocar na cadeia se eu não pagar seus impostos.

A principal diferença é o consentimento.

O individualista americano Albert Jay Nock foi o principal condutor do pensamento de Oppenheimer para os Estados Unidos. Ele capturou o sentimento central de seu mentor no livro *Our Enemy, The State*, no qual Nock observa: “Tomando o estado, onde quer que seja encontrado, adentrando em sua história a qualquer momento, não se vê como diferenciar as atividades de seus fundadores, administradores e beneficiários daqueles de uma classe criminosa profissional”.

A perspectiva de “adentrar a história do estado” atraiu muitos teóricos políticos, porque se relaciona diretamente com a natureza do estado e se ele é legítimo. Por sua vez, isso aborda a questão de porque as pessoas obedecem ao estado. Muitas pessoas parecem consentir com a presença do estado, enquanto reclamam sobre quão corrupto é o sistema e os padrões duplos na lei. Mesmo aqueles que consideram a maioria das leis injustas parecem acatá-las, mesmo não sendo explicitamente forçados a fazê-lo. Mas por quê?

Examinar as raízes do estado é o ponto de partida de uma resposta. Em geral, existem quatro teorias básicas e às vezes sobrepostas

de como um estado se origina. Cada teoria traz implicações diferentes para a relação do estado com a sociedade e a legitimidade que reivindica.

A primeira teoria é sobrenatural. Sustenta que o estado existe pela vontade de Deus ou algo equivalente. Este é o direito divino de reis ou governantes, e a teoria muitas vezes resulta em uma teocracia. Membros menores da sociedade – que presumivelmente também são colocados em suas posições por Deus – devem lealdade aos líderes ungidos, como parte de seu dever para com Deus. Uma igreja estabelecida às vezes atua como um braço do estado, com líderes religiosos reforçando a legitimidade divina do governante.

A segunda teoria de como um estado se origina baseia-se em uma explicação mais naturalista. O estado é uma instituição espontânea que surge do ato da comunidade, argumenta-se. A pessoa e a propriedade dos indivíduos exigem proteção, e seus contratos exigem um mecanismo de execução. Isso faz com que uma autoridade superior evolua para prestar os serviços necessários, atuando como policial e árbitro de disputas. A sociedade paga ao estado da mesma maneira que paga a um empreiteiro pela prestação de um serviço valioso. De acordo com a teoria do consentimento, nenhuma linha rígida distingue o estado da sociedade, porque ambos estão engajados em um empreendimento cooperativo.

A terceira e quarta teorias envolvem conflito. A terceira teoria afirma que o estado surge devido à guerra interna dentro de uma sociedade. Karl Marx popularizou essa visão, analisando o estado como parte da luta de classes, através da qual os capitalistas controlam e exploram os trabalhadores; isto é, os capitalistas usam o estado – ou se unem ao estado – para oprimir os trabalhadores. Para Marx, o estado expressa e protege uma classe da sociedade às custas de outra, e esta não deve qualquer lealdade a seus opressores. De fato, o dever dos trabalhadores é resistir e se rebelar.

A quarta teoria das origens do estado aponta para conflitos externos em que uma tribo conquista outra. A tribo vitoriosa forma a classe alta dentro da sociedade resultante, e a tribo conquistada paga tributo por meio de obediência e riqueza.

Dentro do liberalismo clássico, as duas teorias que lutaram pelo domínio são a teoria do consentimento, pela qual o estado evolui naturalmente a partir das necessidades da sociedade, e a teoria da conquista, pela qual o estado está em constante guerra contra a(s) classe(s) não

privilegiada(s) da sociedade. Estas não são apenas suposições históricas. São também abordagens analíticas para se o estado pode ou não reivindicar legitimidade.

As teorias do consentimento e da conquista do estado

Se o estado governa com o consentimento da sociedade e fornece um serviço necessário, então o argumento contra a revolução – na forma das criptomoedas ou em nome de qualquer outra coisa – é consideravelmente enfraquecido. É provável que o sistema monetário seja visto como necessitando de uma reforma considerável, em vez de ser eliminado.

Na teoria do consentimento do estado, o filósofo inglês do século XVII John Locke se destaca por meio de seus *Dois Tratados sobre o Governo*. A filósofa americana contemporânea Karen Vaughn observa a partir de seu *Segundo Tratado*: "Locke argumenta o caso dos direitos naturais individuais, o governo limitado dependendo do consentimento dos governados, separação de poderes dentro do governo e, mais radicalmente, o direito das pessoas dentro da sociedade de depor governantes que não cumprem sua parte no contrato social". O trabalho de Locke, sobre o qual as revoluções francesa e americana se basearam, continua sendo uma pedra de toque da teoria do consentimento para o governo limitado dentro do liberalismo clássico.

Locke acredita que Deus deu o mundo a todos os homens em comum e justifica a propriedade privada – a apropriação de um bem comum para uso pessoal – argumentando que cada homem tem um direito de propriedade sobre sua própria pessoa. Com base na autopropriedade, Locke argumenta: "O trabalho de seu corpo e o trabalho de suas mãos, podemos dizer, são propriamente dele. O que quer que ele remova do estado que a natureza forneceu e o deixou, ele misturou seu trabalho e juntou a ele algo que é seu, e assim o torna sua propriedade". Até agora, isso não parece sugerir que o estado, ao contrário dos indivíduos, produza riqueza ou valor.

Locke então postula que a necessidade de proteger "vida, liberdade e propriedade" leva os homens a formar um governo. Uma das principais razões pelas quais o estado surge é como um escudo contra a confusão quanto aos títulos de propriedade e outros conflitos, que ocorrem quando os indivíduos acumulam e competem por riqueza em um

mundo de escassez. Por meio de um contrato social explícito, os homens dão ao estado o direito de julgar as disputas. De sua parte, o estado se compromete a garantir a reivindicação de propriedade dos homens – por meio de leis de herança, por exemplo. Locke rejeita a afirmação de que o consentimento prestado ao estado pelos membros iniciais da sociedade pode vincular as gerações futuras, no entanto. Em vez disso, ele desenvolve uma doutrina de consentimento tácito pela qual as pessoas que não consentiram explicitamente ainda são obrigadas a aceitar a autoridade do estado. Diz-se que cada pessoa que vive em sociedade e desfruta de seus benefícios concorda com as regras pelas quais um estado limitado governa.

A retirada do consentimento tácito é possível. Um homem pode renunciar a sua propriedade e deixar a comunidade. Enquanto ele permanecer, no entanto, ele aceita implicitamente a autoridade do estado. Afinal, como argumenta Locke, o "bom título" de sua propriedade veio do estado, que facilitou sua justa transferência. Um argumento semelhante pode ser feito sobre a riqueza acumulada em virtude de um contrato: o contrato tem validade devido ao contexto legal fornecido pelo estado. Somente quando o estado deixa de cumprir sua parte no contrato social é que se justifica a rebelião contra sua autoridade. Caso contrário, o estado e a sociedade são parceiros.

A teoria da conquista do estado contrasta fortemente com o modelo lockeano e é a teoria preferida pelos anarquistas individualistas. Ele tenta fundamentar o estado primitivo em fatos históricos, em vez de conjecturas políticas. Uma expressão comum da teoria da conquista é a seguinte: tribos agrícolas se estabelecem e se tornam dependentes de áreas específicas de terra. Nômades itinerantes fazem guerra às tribos mais sedentárias pelos benefícios econômicos que vêm da pilhagem e do saque. Os nômades começam matando e arrasando, mas descobrem que é do seu interesse econômico de longo prazo escravizar e exigir tributos. Por que roubar por uma única estação quando é possível roubar para sempre? Este é o modelo de conquista simplista para explicar como surgiu o estado e sua relação com a sociedade.

Em *Our Enemy, The State*, Nock defende a teoria da conquista do estado em bases históricas. Em *For A New Liberty*, Rothbard apresenta uma versão modificada da teoria. Ele afirma que a conquista foi a gênese típica do estado, mas admite que alguns estados podem ter evoluído de maneira diferente. Mas mesmo um estado que emergiu de um

contrato social explícito, argumenta ele, não poderia vincular novas gerações por meio de consentimento tácito, porque uma atribuição de direitos naturais requer um contrato explícito. Como não existe renovação geracional do contrato, qualquer estado atual não tem legitimidade.

Ao defender a teoria da conquista, tanto Nock quanto Rothbard se apoiam fortemente em Oppenheimer, que sustenta que o estado consiste em pessoas que desejam satisfazer seu "impulso econômico" através dos meios políticos – através do uso da força. Oppenheimer postula seis estágios pelos quais um grupo conquistador normalmente passa para se tornar um estado:

- Primeiro, um grupo guerreiro ataca e saqueia uma comunidade vulnerável para roubar riqueza em vez de produzi-la por conta própria. Os ataques vikings na costa britânica são um exemplo.
- Em segundo lugar, a comunidade vitimizada deixa de resistir ativamente; às vezes é feito um acordo explícito entre os agressores e as vítimas. Os saqueadores passam a saquear apenas o excedente, deixando suas vítimas vivas e com comida suficiente para garantir a produção de riqueza futura a ser saqueada repetidamente. Eventualmente, os dois grupos reconhecem interesses mútuos, como proteger as plantações de terceiras partes externas.
- Terceiro, as vítimas prestam homenagem aos invasores, eliminando a necessidade de qualquer violência.
- Quarto, os dois grupos se fundem territorialmente e vivem juntos na mesma área.
- Quinto, o grupo belicoso assume a autoridade para arbitrar disputas, o que envolve o monopólio do uso da força.

Oppenheimer descreve o último estágio em que ambos os grupos desenvolvem o "hábito de governar". Em seu capítulo "A Gênese do Estado", ele explica: "Os dois grupos, separados, para começar, e depois unidos em um território, são inicialmente apenas colocados um ao lado do outro, depois são desmembrados um pelo outro. Misturam-se, unem-se, amalgamam-se à unidade, nos costumes e hábitos, na fala e no culto. Logo os laços de relacionamento unem os estratos superiores e inferiores." Os estratos superiores eram chamados de "classe de mestres."

O estado, que se originou da conquista externa, evolui para uma agência de conquista interna pela qual as camadas superiores do estado

utilizam os meios políticos para se beneficiar economicamente às custas das camadas inferiores de produtores. Nessa visão, o estado surge e se mantém como parasita e inimigo da sociedade. Ainda assim, em qualquer que seja o caminho que leve ao surgimento de um estado uma questão permanece: por que as pessoas aceitam a autoridade do estado sobre suas vidas, suas propriedades e o futuro de suas famílias?

Servidão Voluntária

A força é geralmente o último recurso que o estado introduz quando outros métodos de persuasão, como o apelo ao patriotismo, não funcionam. Afinal, a presença da força aberta poderia colocar em questão a legitimidade do estado. Para evitar a desobediência ou a rebelião, o estado tenta justificar-se aos olhos da sociedade para que possa garantir as vantagens da violência sem incorrer em seus perigos. Nenhuma análise da relação entre estado e sociedade está completa sem examinar a questão da legitimidade.

Um ensaio do século XVI intitulado "Discurso da Servidão Voluntária" do jurista francês Étienne de La Boétie é uma discussão inicial de uma questão inquietante. Por que as pessoas obedecem a leis injustas? La Boétie pergunta: "Se um tirano é um homem e seus súditos são muitos, por que eles consentem em sua própria escravização?" Corretamente ou não, La Boétie não acredita que o estado governe principalmente pela força. Afinal, há muito mais pessoas na sociedade do que agentes do estado. Se mesmo uma pequena porcentagem da população se recusa a obedecer a uma lei, então a lei se torna inaplicável; a tirania é automaticamente derrotada se as pessoas retirarem seu consentimento. No entanto, a maioria das pessoas obedece sem ser forçada a fazê-lo. La Boétie desenvolve uma explicação; ele chama isso de "servidão voluntária".

O Discurso circulou pela primeira vez privadamente na França (por volta de 1553) em um cenário de guerra estrangeira e conflito interno. Os estados-nação europeus estavam em ascensão, e os monarcas entraram em conflito não apenas entre si, mas também com seus próprios cidadãos, de quem exigiam muito dinheiro e obediência. O século XVI deu origem à tirania que levou à Revolução Francesa séculos depois.

Nascido em uma família abastada e politicamente conectada, La Boétie escapou do analfabetismo, miséria e doenças que se abateram

sobre a maioria de seus compatriotas. A fome era tão comum na França que os homens esculpiam cruzes no pão recém-assado para simbolizar a sacralidade da comida. Pragas irromperam repetidamente. Enquanto o camponês lutava para sobreviver, os impostos estaduais consumiam um terço ou mais de sua renda, com os dízimos da igreja absorvendo outro décimo. Grupos itinerantes de soldados roubavam à vontade e sequestravam filhos jovens para preencher suas fileiras. A França era uma monarquia absoluta, o que significava que o poder nacional não era distribuído, mas ficava com o rei e era administrado por meio de nomeações. Para arrecadar dinheiro para a guerra e o luxo, o rei vendia títulos aos “nouveau riche”, que formavam uma nova aristocracia com notório desprezo pelas classes mais baixas. Enquanto isso, as fileiras de advogados aumentavam enquanto administravam burocracias para alimentar o apetite de um estado em crescimento.

Por que o homem comum obedeceu a um sistema que o tratou tão miseravelmente e foi claramente manipulado contra ele? Para garantir isso, o monarca foi ungido por Deus e abençoado pela Igreja Católica dominante, mas a ascensão do protestantismo na França – os huguenotes – fez com que um segmento crescente da sociedade não reconhecesse a divindade do rei. Havia também lealdades provinciais que competiam com as nacionais. A maioria dos franceses dava fidelidade primária à província de seu nascimento e não à nação ou ao rei, e as províncias variavam amplamente em costumes, práticas religiosas e linguagem. Essas diferenças dividiram a nação. Também e com razão, o rei temia que potências estrangeiras se alinhassem contra ele com províncias rebeldes. Uma tempestade perfeita entre o estado e a sociedade parecia estar se formando.

O Discurso provavelmente foi escrito enquanto La Boétie era estudante de direito na Universidade de Orléans, famosa pela atividade huguenote. De fato, um de seus professores seria mais tarde queimado na fogueira por heresia. O ensaio em si era uma resposta a um evento específico – a Revolta de Gabelle em Bordeaux. O Gabelle era um imposto muito odiado sobre o sal, que não era apenas uma necessidade humana, mas também um monopólio estatal. Os manifestantes mataram o diretor geral do Gabelle junto com dois de seus oficiais. Em retaliação, 140 plebeus foram mortos, muitos outros foram chicoteados e multas exorbitantes foram impostas.

La Boétie era um observador perspicaz da sociedade. Quando o povo finalmente se rebelou, ele observou e se perguntou por que o estado foi capaz de fazer quase tudo o que queria por tanto tempo, não importa o quão tirânico. Ele assistiu de perto também depois que a Revolta de Gabelle foi anulada. Por que as pessoas não se levantaram novamente, ele se perguntou, desta vez en masse? Por que a sociedade tolerava o estado? *O Discurso* foi a resposta de La Boétie.

Nele, o autor conclui que a obediência coletiva da sociedade vem de "um vício para o qual nenhum termo pode ser encontrado suficientemente vil, que a própria natureza repudia e nossas línguas se recusam a nomear". Ele chama isso de "servidão voluntária". É um vício porque contradiz a natureza humana; na verdade, até os animais brutos lutam para se libertar quando apanhados em uma armadilha. Cada homem recebe sua própria capacidade de raciocinar, argumenta La Boétie, e a virtude reside no cultivo de cada pessoa de sua própria independência inata. Mas a habilidade do homem de fazê-lo exigiu a morte da tirania, que é a antítese da independência individual. A defesa do tiranicídio não era novidade para a teoria europeia, mas La Boétie adota um viés diferente. A maneira de "matar" um tirano é destruir seu poder através da resistência não-violenta. Dessa maneira, o povo não mata um homem, mas a própria tirania. A liberdade exige apenas que um número suficiente de pessoas retire seu consentimento e cooperação.

> Aquele que assim domina você tem apenas dois olhos, apenas duas mãos, apenas um corpo [...]; ele realmente não tem nada mais do que o poder que você confere a ele para destruí-lo. Onde ele conseguiu olhos suficientes para espioná-lo, se você mesmo não os forneceu? Como ele pode ter tantos braços para bater em você, se ele não os empresta contigo? Os pés que pisoteiam suas cidades, de onde ele os tira senão dos teus?

La Boétie dirige-se diretamente ao camponês francês. "Vocês entregam seus corpos ao trabalho duro para que ele [o tirano ou o estado] possa se entregar a seus deleites e chafurdar em seus prazeres imundos; vocês se enfraquecem para torná-lo mais forte e mais poderoso para mantê-los sob controle". Por que obedecer?

La Boétie explora as principais formas pelas quais os engenheiros estatais consentem com a sociedade.

As gerações que nasceram "sob o jugo e depois foram nutridas e criadas na escravidão" aceitam sua condição como natural. É o caminho do mundo. Assim, La Boétie considera o costume como a primeira explicação da servidão voluntária. As pessoas acreditam que a vida sempre foi assim; a vida sempre será assim; e é preciso um grande esforço para introduzir uma nova visão a eles.

O autor e teórico francês Michel de Montaigne, que era o melhor amigo de La Boétie, dramatizou o incrível poder da tradição em seu ensaio "Do Costume". Abre com as palavras:

> Parece ter tido uma apreensão correta e verdadeira do poder do costume, quem primeiro inventou a história de uma camponesa que, acostumada a brincar e carregar um bezerro nos braços, e continuando diariamente a fazê-lo como cresceu, obteve isso por costume, que, quando crescido para ser um grande boi, ela ainda era capaz de suportar.

Mas, argumenta La Boétie, algumas pessoas sempre tentarão se livrar "do jugo", talvez porque "se lembrem de seus ancestrais e de seus antigos costumes". Conscientes da história, comparam o passado com o presente e ousam ansiar por um futuro melhor. "Estes são os que, tendo suas próprias mentes boas, os treinaram ainda mais pelo estudo e aprendizado. Mesmo que a liberdade tivesse desaparecido inteiramente da terra, tais homens a inventariam".

Depois que a maioria se acostuma à obediência automática, o principal desafio do tirano é reduzir a dissidência silenciando os poucos que tentam livrar-se do jugo. Dois meios básicos de fazer isso são controlar a imprensa e monopolizar a educação para que as pessoas não comparem o passado com o presente e percebam o quanto mais é possível no futuro. Com um forte controle da informação, o estado pode inculcar a crença de que age em prol do bem-estar público para manter a paz, o patriotismo e a tradição. Pode convencer as pessoas de que incorpora o bem público. A *lavagem cerebral* é outra razão pela qual as pessoas obedecem.

O estado, então, reforça sua imagem maior que a vida por meio de um processo de *mistificação*: isto é, tenta parecer maior do que a mera reunião de seres humanos em suas fileiras. Os governantes se alinham com a religião, são coroados por oficiais da Igreja, realizam cerimônias pomposas, juram proteger a nação, apelam à autoridade de um

documento fundador e assim por diante. Os agentes do estado estão vestidos com uniformes; são construídos monumentos ao poder estatal e aos líderes do passado; os rituais do ofício são ostensivamente exibidos; e manifestações da autoridade do estado, como tribunais, estão alojadas em edifícios imponentes.

Esta é mais uma razão pela qual as pessoas prestam obediência automática: mistificação. Depois que uma imprensa regulamentada e um sistema escolar os convenceu de que a autoridade do governante é legítima, a mistificação do poder do estado os leva um passo adiante.

Eles ficam amedrontados, intimidados e até temerosos.
Algumas pessoas ainda serão difíceis de convencer, no entanto. Aqueles que não obedecerem por costume, lavagem cerebral ou admiração podem muito bem ser comprados. E, assim, o governante também se engaja na generosidade. La Boétie aponta para as distrações patrocinadas pelo estado que servem como "ópios". Fascinado pelo prazer, o povo não percebe sua própria escravização. Outras vezes, os governantes literalmente alimentam o povo distribuindo estoques de alimentos. "E então todos gritam descaradamente: 'Longa vida ao rei!'", comenta La Boétie com desdém. "Os tolos não perceberam que estavam apenas recuperando uma parte de sua própria propriedade, e que seu governante não poderia ter dado a eles o que estavam recebendo sem primeiro tê-lo tirado deles." Ao fornecer pão e circo – bem-estar do estado e distrações populares – as pessoas são *subornadas* para que abdiquem de sua liberdade.

O suborno direto perde importância, no entanto, ao lado de uma forma indireta que La Boétie chama de "a mola mestra e o segredo da dominação, o suporte e a base da tirania". Isso é suborno institucionalizado pelo qual milhões de pessoas são empregadas em empregos estatais e recebem fundos de impostos com os quais pagam suas contas. Esses funcionários do estado "se agarram ao tirano" e oferecem sua lealdade. Alguns funcionários do estado, como policiais, tornam-se as mãos do estado, alcançando toda a sociedade para implementar leis e políticas. Intelectuais apoiados por impostos, como professores universitários, tornam-se as vozes do estado, defendendo suas políticas. Outros ainda, trabalhando como escriturários ou burocratas menores, fazem a máquina diária do estado funcionar.

Ao longo de gerações, uma vasta nova classe de pessoas emerge dos funcionários do estado: pessoas que servem aos governantes em troca de um salário financiado por impostos e outros benefícios. Esses

funcionários públicos destroem voluntariamente sua própria liberdade e a de seus vizinhos. E o fazem sem reflexão porque a força do costume os leva a acreditar que as coisas sempre foram e sempre serão assim.

A solução de La Boétie para a servidão voluntária é que as pessoas retirem seu consentimento e cooperação do estado. La Boétie aconselha o homem comum: “Eu não peço que você coloque as mãos sobre o tirano para derrubá-lo, mas simplesmente que você não o apoie mais; então você o verá, como um grande colosso cujo pedestal foi arrancado, cair de seu próprio peso e quebrar em pedaços.” La Boétie é amplamente reconhecido como uma das primeiras vozes de desobediência civil e resistência não-violenta contra a autoridade.

Se ele estiver correto, se a liberdade é um desejo humano natural, então a própria natureza argumenta a lógica de não cooperar com a tirania. Algo dentro dos seres humanos e até dos animais resiste à tensão de uma coleira. Em vez de quebrar a tensão atacando aqueles que detêm os reinados, La Boétie disse às pessoas que deixassem a tensão afrouxar; deixe a ponta da coleira cair. As pessoas devem se recusar a se defender violentamente ou a se submeter.

Eles devem simplesmente dizer “não”.

Estado, Sociedade, Obediência e Cripto

Para repetir: os conceitos e realidades de estado, sociedade e obediência são o contexto em que o Bitcoin nasceu e no qual as criptomoedas agora operam. Eles também definirão seu futuro.

O estado deve tirar a riqueza da sociedade para existir. As criptomoedas não são apenas uma nova e rica fonte de riqueza para saquear, mas também uma forte concorrente da fonte atual mais lucrativa do estado: o monopólio monetário. O objetivo do estado é acessar a bonança das criptomoedas *e* preservar o monopólio monetário. Sendo inteiramente orientado para fins, o estado usará todos e quaisquer meios à sua disposição para atingir esse objetivo. As estratégias já em exibição incluem:

Propaganda: as criptomoedas estão ligadas a crimes como terrorismo, resgates e tráfico de seres humanos de uma maneira que faz com que esses crimes pareçam ser os usos predominantes. A ligação serve a pelo menos dois propósitos. Isso cria uma justificativa para o estado agir contra a criptomoedas e reduz qualquer reação indesejada por parte

do público geral. Em vez disso, o público gritará: “Deverá haver uma lei”.

O Uso da Força: Como o próprio estado é uma força institucionalizada, esta é sua estratégia final em situações em que a obediência não pode ser obtida de outras maneiras. E as criptomoedas são irremediavelmente desobedientes. A estratégia de violência ou conquista empregada pelo estado geralmente se acelera por etapas:

- O estado saqueia. A privacidade das transferências de blockchain e o viés antiestatista da comunidade cripto tornam essa opção problemática. Indivíduos e corretoras vulneráveis são atacados e seus fundos são confiscados, mas grande parte das criptomoedas permanece fora de alcance.
- O estado chega a um acordo com usuários de cripto compatíveis. As corretoras centralizadas que concordam em cumprir os regulamentos bancários e os requisitos de relatórios são licenciadas e se tornam corretoras comparsas.
- O estado protege as corretoras de compadres dos concorrentes. Indivíduos que funcionam fora das zonas cripto regulamentadas – e especialmente corretoras descentralizadas – tornam-se alvos. Atacar esses “inimigos externos” beneficia tanto o estado quanto as corretoras obedientes.
- O estado tenta transformar as criptomoedas em um novo tipo de dinheiro fiduciário. Por meio de instituições financeiras, o estado pode imitar a dinâmica das criptomoedas de forma a reproduzir o monopólio monetário de que goza com a moeda fiduciária. Moeda digital que não usa blockchain pode ser oferecida, por exemplo; isso permitirá uma inflação lucrativa e que o estado rastreie todas as transações de volta para um usuário.

Enquanto passa pelos estágios do uso da força, o estado se envolverá em um duplo pensamento ativo, semelhante ao slogan “Uma guerra para acabar com todas as guerras”. As corretoras centralizadas serão apresentadas como forma de garantir a segurança do patrimônio dos usuários, por exemplo, ainda que o maior perigo para a sua riqueza seja o sistema de banco central que as corretoras espelham.

A propaganda contra as criptomoedas não regulamentadas continuará, pois, na presença de alternativas, o estado precisa que o público continue aceitando o monopólio monetário. Muitas pessoas vão fazê-lo

através do costume. Alguns farão isso por causa de lavagem cerebral pela mídia cúmplice que se concentra em qualquer irregularidade dos usuários de criptomoedas. Enquanto isso, o estado mistificará suas próprias atividades, auxiliado pelo fato de que poucas pessoas entendem a tecnologia das criptomoedas ou da moeda digital. O primeiro – se não regulamentado – será diminuído como inseguro, criminoso e falso. O último – sob controle do estado – será considerado seguro, legítimo e forte.

As criptomoedas que se recusarem a serem regulamentadas continuarão sendo o dinheiro da sociedade – ou seja, o dinheiro de indivíduos que interagem livremente e em seu próprio interesse para benefício mútuo. Continuarão a produzir riqueza. Em virtude da cripto ser orientada para os meios, como a sociedade, ela evoluirá para diversos fins com apenas os meios sendo previsíveis: não-violência e consentimento. O conflito entre dinheiro privado e dinheiro fiduciário persistirá porque os dois têm dinâmicas fundamentalmente antagônicas que se ameaçam. Um dos principais campos de batalha será a opinião pública.

Nesse campo de batalha, o maior desafio que o mundo cripto enfrenta é convencer um número suficiente de pessoas a simplesmente dizer “não”.

Teoria Cripto de Classe e Lei de Livre Mercado

A teoria de classe fundamenta o livre mercado e as criptomoedas: o estado versus a sociedade. O Bitcoin foi projetado para contornar um sistema bancário central que serve à classe política em detrimento da econômica. Como inimiga do estado, a criptomoeda é uma aliada da sociedade.

Guerra de Classes e Cripto

Muitas pessoas assumem que qualquer coisa relacionada a bancos e finanças expressa os interesses de classe dos capitalistas versus o homem comum. O oposto é verdadeiro, mas a confusão é compreensível. A palavra "capitalismo" é comumente aplicada ao capitalismo de compadrio nos dias de hoje – isto é, um arranjo econômico pelo qual algumas empresas desfrutam de um relacionamento próximo e mutuamente benéfico com funcionários do estado e recebem tratamento privilegiado. Um "capitalista" tradicional é aquele que possui e usa bens de capital, permanecendo na sociedade sem vínculo com o estado; esse arranjo econômico às vezes é chamado de "capitalismo laissez-faire". É uma expressão do livre mercado e é um benefício para o homem comum, porque o capitalismo laissez-faire atua como um motor de prosperidade.

Os bancos centrais e a maioria das instituições financeiras expressam o capitalismo de compadrio. O capitalismo laissez-faire expressa o livre mercado. Assim, uma afirmação mais específica do conflito de classes é o capitalismo de estado e compadrio versus sociedade e capitalismo laissez-faire. Nesse conflito, a criptomoeda cai claramente do lado da sociedade. A lealdade de classe da criptomoeda é evidente pelos notáveis paralelos entre sua forma e função e os da sociedade. Os paralelos incluem:

- O indivíduo é o locus do poder.
- Ambos são descentralizados até o nível do indivíduo.
- Voluntarismo é o modo de operação.
- Sua finalidade é facilitar as trocas, principalmente econômicas.
- As trocas ocorrem somente com o consentimento de todos os envolvidos.

- Terceiras partes confiáveis são desnecessárias.
- A privacidade é preservada, caso os participantes assim o desejem.
- Não há barreira artificial à entrada.
- Nenhum deles é detentor de um ponto fraco em que todo o sistema esteja vulnerável.
- A riqueza está sendo constantemente criada.
- Riqueza e status são baseados em labuta.
- As trocas não são baseadas em ideologia ou política.
- Reputações são importantes.
- O estado é o inimigo da classe.

Por outro lado, a forma e a função do estado são antitéticas à criptomoeda e ao livre mercado.

- O estado é o locus do poder.
- Todo o poder é centralizado em burocracias.
- A coerção é seu modo de operação.
- O objetivo do estado é manter sua própria existência.
- Transferências forçadas de riqueza e poder são feitas em benefício do estado.
- É a terceira parte última.
- A privacidade é desaprovada e prejudicada a cada passo.
- Barreiras à entrada são erguidas, às vezes chegando a proibições.
- Quem está no poder é o ponto fraco do sistema.
- Nenhuma riqueza é criada.
- Riqueza e poder são baseados na política.
- A riqueza é acumulada por meio de roubo e privilégio.
- A reputação não é necessária e menos importante que o status.
- A sociedade é a inimiga da classe.

Outro teste decisivo para saber se a criptomoeda serve ao estado ou à sociedade está enraizado nas respostas a duas perguntas sobre dinheiro. #1. Quem o emite? O dinheiro fiduciário é emitido pelo estado ou por uma autoridade controlada pelo estado, sendo a concorrência proibida por lei. As criptomoedas são emitidas por empreendedores que

competem vigorosamente entre si pela aceitação popular. #2. As pessoas podem optar por usar a moeda ou não? O estado exige que as pessoas aceitem seu fiat como moeda legal. A cripto deixa a decisão para o indivíduo.

Talvez a maior ameaça à criptomoeda não regulamentada seja o esforço do estado para mudar a forma e a função da criptomoeda para que ela não mais expresse e enriqueça a sociedade, mas expresse e enriqueça o estado. O estado queria esculpir a criptomoeda em sua própria imagem por meio de emissão estatal, regulamentação e outras medidas para que se tornasse um tipo de criptomoeda fiduciária. Isso não pode ser feito; a blockchain não pode ser centralizada sob uma única autoridade. Nenhuma mistura de forças inerentemente antagônicas é possível. Não é sequer claro que criptos estatais e de livre mercado possam coexistir.

O estado continuará tentando forjar uma criptografia bastarda, no entanto, até que esteja convencido de que os esforços são inúteis. Neste ponto, a criptomoeda deixará de ser vista como uma oportunidade e será vista como um perigo. A própria existência de criptomoedas de livre mercado invade uma fonte insubstituível de poder estatal – a emissão de dinheiro. A criptomoeda tem a capacidade de enfraquecer essa fonte de poder e, talvez, destruí-la.

Os recursos de criptografia que enfraquecem o estado incluem:

- As transferências peer-to-peer negam riqueza evitando os bancos centrais através dos quais o fluxo financeiro é controlado.
- A privacidade cripto atrapalha a campanha de controle social do estado. Os dados das instituições financeiras que informam sobre seus clientes são vitais para a capacidade do Estado de impor controle social e econômico.
- A privacidade também evita a centralização do estado. O estado quase pode ser definido como a centralização do poder para beneficiar a elite.
- A existência da cripto levanta a questão de saber se o estado é necessário. Se o livre mercado pode assumir tão facilmente uma função essencial do estado – a emissão e circulação de moeda – então por que não pode assumir outras, ou todas?

A cripto é o dinheiro da sociedade; não pode e não serve ao estado.

A aplicação da lei como ferramenta da guerra de classes

> O poder tributário coercitivo do governo cria necessariamente duas classes: os que criam e os que consomem a riqueza expropriada e transferida por esse poder. Aqueles que criam a riqueza naturalmente querem mantê-la e dedicá-la aos seus próprios propósitos. Aqueles que desejam expropriar procuram formas cada vez mais inteligentes de adquiri-lo sem incitar resistências. Uma dessas formas é a divulgação de uma elaborada ideologia de estatismo, que ensina que as pessoas são o estado e que, portanto, eles só estão pagando a si mesmos quando pagam impostos. Os oficiais do estado e os intelectuais do tribunal nas universidades e os meios de comunicação fazem de tudo para que as pessoas acreditem nessa história fantástica, incluindo a criação de escolas. Infelizmente, a maioria das pessoas passa a acreditar.
> – Sheldon Richman

Uma das armas mais poderosas que o estado possui na luta de classes que trava contra a sociedade é a imposição da lei, incluindo a legislação e o sistema judicial através do qual o estado afirma seus privilégios de classe. A lei é parte integrante do monopólio do estado sobre a força e sua capacidade de coagir a transferência de riqueza da sociedade para suas próprias mãos. Sem o monopólio da imposição da lei, é difícil imaginar como o estado poderia vencer o conflito de classes, porque a sociedade desfruta das enormes vantagens de ser produtiva, inovadora e enérgica.

O estado investe imenso tempo e imensas quantias de dinheiro para convencer a sociedade de que a imposição da lei é uma proteção, não uma ameaça. À medida que um estado se aproxima do totalitarismo, porém, torna-se mais difícil manter esse engano porque suas armas – isto é, as indústrias de imposição da lei – tornam-se mais visíveis.

Uma das últimas ferramentas que o Estado usa para manter a legitimidade antes de começar a usar armas é o argumento N.H.A: não há alternativa. O estado incita o medo de um terrível inimigo – terroristas,

talvez – e então assegura à sociedade que são necessários guardas armados nos aeroportos, câmeras de vigilância e uma força policial militarizada. Além disso, não há alternativa. Ou melhor, a única alternativa é o terrorismo. Muitos acreditarão nessa falsa escolha e aceitarão o menor de dois males.

Felizmente, existe uma alternativa: a lei do livre mercado.

Lei de livre mercado

> Há uma distinção importante entre legislação e lei. Legislação é a lei que vem da ação política. […] A lei é mais geral no sentido de que a legislação é uma forma de lei, mas a lei também pode ser o tipo de lei que evolui através da interação humana. Na Inglaterra e nos Estados Unidos, muitas vezes somos chamados de países de 'common law' e isso porque uma boa parte e, de fato, a maior parte de nossa lei surgiu por meio de um processo evolutivo que não envolveu a ação de representantes políticos.
> – John Hasnas

Deveria haver uma lei. O significado desta afirmação depende da definição de "lei". O estado trata a palavra como sinônimo de legislação ou lei estatutária, que é a lei que resulta de um processo político. Qualquer pessoa ou grupo que detenha poder suficiente pode aprovar legislação e usar a aplicação da lei para impô-la à sociedade. Trata-se de um modelo centralizado e redutor pelo qual uma classe superior determina como a classe inferior deve se comportar. O efeito das decisões da classe alta flui verticalmente para a vida das pessoas da classe baixa. O único perigo para um sistema piramidal é que os seres humanos agem em seu próprio interesse, e a lei legislada provavelmente reflete os interesses dos políticos, e não os das pessoas a quem é imposta. O sistema é uma fórmula para a corrupção e uma porta de entrada para o estado se expandir cada vez mais profundamente na sociedade.

Pode haver lei viável sem o Estado? Anarquistas e defensores do governo limitado têm debatido essa questão há séculos, com muitas vozes do livre mercado concluindo que a lei deve emanar do estado da mesma maneira que eles acreditam que o dinheiro deve. O direito é uma necessidade humana sem a qual a sociedade civil dificilmente durará muito. Se o livre mercado não pode fornecer esse bem essencial, então

o anarquismo falha e o governo limitado é a alternativa mais prática. A sociedade se tornará um parceiro júnior do estado. A eterna luta entre a Liberdade e o Poder sobre a qual Rothbard escreveu terminará com o Poder declarando vitória.

É uma abordagem útil começar definindo o termo "lei". Lei é um termo mais geral do que "legislação", que é meramente uma forma de lei; o termo geral refere-se a qualquer código ou conjunto de regras que governam a interação humana. "Governança" não implica em estado.

Pode haver lei sem um estado? A resposta: "sim, pode", e por um motivo: a sociedade precede o estado, que necessariamente surge da reunião de seres humanos que buscam interação. A sociedade precede tanto o estado quanto a lei.

Outra razão pela qual a lei de livre mercado pode existir é porque ela já existe.

Uma forma popular de lei de livre mercado é chamada de lei comum ou consuetudinária. Este é um conjunto de regras baseadas em precedentes que evoluem ao longo do tempo para resolver disputas em uma comunidade específica. Não é preventivo, mas reativo. Quando uma disputa irrompe, as partes vão a um terceiro imparcial ou a uma assembleia da comunidade para que seus casos sejam ouvidos. Em uma comunidade rural, por exemplo, se um homem acusa outro de roubar um animal de fazenda, então o árbitro avalia o caso e aplica um padrão comunitário que surgiu de casos semelhantes no passado. Uma vez que os próprios juízes podem estar envolvidos em uma futura disputa comunitária, eles têm interesse em infundir o processo com bom senso.

Isso é lei popular. É uma lei descentralizada que não tem a ampla aplicação das leis federais porque é adaptada às circunstâncias e padrões locais. Uma vila de pescadores quase certamente desenvolveria regras de comportamento diferentes de uma cidade de mineração, por exemplo. As regras que regem a comunidade de criptomoedas seriam diferentes das regras da indústria da construção. Enquanto o objetivo for preservar a interação pacífica e corrigir as violações, não há certo ou errado no conteúdo específico da lei.

O estudioso jurídico John Hasnas explica:

> O direito consuetudinário é o tipo de direito que evolui quando surgem disputas. [...] Com o passar das décadas e séculos, à medida que as coisas evoluem, o tomador de decisões torna-se cada vez mais especializado, e quando você

> chega à era normanda na Inglaterra, as decisões são tomadas por júris. Os júris ainda são formados por pessoas comuns do país. […] Em nosso sistema, não se tem tribunais organizados de forma hierárquica até o final do século XIX, então já é 1873 e 1875.

Uma sociedade moderna complexa pode funcionar sem um conjunto homogeneizado de regras que são obrigatórias? A lei fundamentalmente descentralizada pode funcionar dentro de uma estrutura muito maior do que uma vila de pescadores ou uma comunidade rural?

A perspectiva tem sido discutida há séculos.

A Primeira Discussão da Lei de Livre Mercado e Sistemas de Defesa

> Ao nosso redor estão os benefícios quase inimagináveis de mercados, cooperação e tecnologia, mas de alguma forma somos ingênuos se não quisermos canalizar a atividade humana através das rampas de gado do governo. A vasta abundância material e digital que desfrutamos todos os dias é fornecida sem nenhum aparato estatal e, na verdade, o é *apesar* desse aparato. Este mundo privado não faz parte da realidade? O governo é o artifício, e os estatistas são os sonhadores utópicos que imaginam que indivíduos agindo sob a bandeira mágica do governo podem planejar, coagir e coordenar milhões de vidas.
> – Jeff Deist

O liberal clássico do século XIX Gustave de Molinari respeitava o livre mercado tão profundamente que seus colegas se referiam a ele como “a lei da oferta e da demanda transformada em homem”. Muito elogiado em sua época, Molinari caiu na obscuridade. Seu legado deve ser recuperado, no entanto, porque ele levantou uma questão crucial. Por que a segurança é um serviço monopolizado pelo estado e não executado pelo livre mercado, que fornece todos os outros serviços de forma mais eficiente e barata?

Molinari é o primeiro precursor explícito do anarquismo de livre mercado. Rothbard alude a seu ensaio de 1849, “Da produção de segurança”, como “a primeira apresentação em qualquer lugar da história

humana do que agora é chamado de 'anarcocapitalismo' ou 'anarquismo de livre mercado'". O núcleo do anarquismo de Molinari é sua teoria de como a sociedade surge.

> Há duas maneiras de considerar a sociedade. Segundo alguns, o desenvolvimento das associações humanas não está sujeito a leis providenciais e imutáveis. Em vez disso, essas associações, tendo sido originalmente organizadas de maneira puramente artificial por legisladores primitivos, podendo mais tarde ser modificadas ou refeitas por outros legisladores, de acordo com o progresso da *ciência social*. Nesse sistema, o governo desempenha um papel preeminente, pois é sobre ele, guardião do princípio da autoridade, que recai a tarefa cotidiana de modificar e refazer a sociedade.
> Segundo outros, ao contrário, a sociedade é um fato puramente natural. Como a terra em que está, a sociedade se move de acordo com leis gerais preexistentes. Nesse sistema, não existe, estritamente falando, ciência social; existe apenas a ciência econômica, que estuda o organismo natural da sociedade e mostra como esse organismo funciona.

Molinari acredita que os homens formam a sociedade por interesse próprio para satisfazer o mesmo "instinto de sociabilidade", demonstrado por outros animais de alta ordem; a sociabilidade foi construída na natureza do homem da mesma forma que a fome. A sociedade é organizada espontaneamente com o propósito de fazer trocas amplamente definidas; estas são a esfera apropriada do estudo econômico, não da ciência social.

Molinari apresenta três métodos pelos quais qualquer bem ou serviço pode ser produzido.

- O primeiro método é conceder um monopólio a uma entidade privilegiada. Isso é o que acontece quando o estado recebe o monopólio do uso da força e da lei dentro de uma jurisdição. Indivíduos dissidentes são forçados a obedecer, ou são silenciados.

- O segundo método é através de um coletivo que produz um serviço que diz beneficiar a sociedade em geral. A autoridade investida em uma democracia é um exemplo. Essa forma menos centralizada de controle não é menos perigosa para um dissidente.
- O terceiro método é a competição de livre mercado. A autoridade reside com indivíduos que são empresários e clientes. Os indivíduos escolhem livremente fazer negócios ou não.

Todos os serviços e bens devem ser questões puramente econômicas, incluindo segurança e defesa. Como todos os outros serviços que atendem a uma necessidade humana, a segurança é melhor fornecida por um livre mercado, no qual os indivíduos exercem o poder supremo do “sim” ou do “não”. Molinari é o primeiro teórico a apresentar um argumento coeso sobre como os mecanismos de livre mercado podem substituir as chamadas funções essenciais do estado, especialmente a proteção contra agressões. Ele afirma que o mercado também estabelece uma sociedade mais justa do que o governo.

> Essa opção que o consumidor retém de poder comprar segurança onde bem entender provoca uma constante emulação entre todos os produtores, cada produtor se esforçando para manter ou aumentar sua clientela com a atração do barateamento ou da justiça mais rápida, mais completa e melhor.
> Se, ao contrário, o consumidor não é livre para comprar títulos onde quiser, logo se abre uma grande profissão dedicada ao arbítrio e à má gestão. A justiça torna-se lenta e custosa, a polícia vexatória, a liberdade individual não é mais respeitada, o preço da segurança é inflacionado de forma abusiva e repartido de forma desigual, conforme o poder e a influência desta ou daquela classe de consumidores. Os protetores se envolvem em lutas amargas para arrancar clientes uns dos outros. Numa palavra, surgem todos os abusos inerentes ao monopólio ou ao comunismo.

Em suma, *não* deveria haver outra lei; que não a de livre mercado.

Molinari esboça brevemente um plano de como pode ser o serviço econômico de segurança. Para começar, ele se concentraria inteiramente na proteção da pessoa e da propriedade, em vez da proteção do estado ou de um código moral. Isso elimina a grande maioria das leis. Também reduz as guerras constantemente travadas por território por nações que desconsideram as preferências das populações.

A segurança seria um negócio – ou muitos negócios – incluindo forças policiais privadas e serviços de arbitragem. Os clientes em potencial provavelmente fariam uma série de perguntas a um provedor, incluindo uma que Molinari sugere; Será que "qualquer outro produtor de segurança, oferecendo garantias iguais … oferecerá … esta mercadoria em melhores condições?" Em suma, Molinari prevê um sistema de provedores de segurança que funciona da mesma maneira que as seguradoras de hoje. Ele conclui: "Sob um regime de liberdade, a organização natural da indústria de segurança não seria diferente da de outras indústrias".

Uma contrarresposta surge inevitavelmente; lei exige consenso.

Locke sobre o argumento do consenso para o direito

A percepção do problema da necessidade de consenso tem assombrado a questão do estado versus direito privado e justiça. Seu defensor mais persuasivo foi John Locke.

> A chave para… um sistema judicial anarcocapitalista é encontrada no conceito de um "judiciário pessoal". [Atuando como seu próprio juiz.] … O propósito dos tribunais é permitir que os homens resolvam disputas de modo a evitar a resolução violenta, bem como os ciclos de agressão-compensação. Considerar as decisões dos tribunais como legítimas é a única maneira de os litigantes evitarem ações *judiciais pessoais*.
> – Karl T. Fielding, "The Role of Personal Justice in Anarcho Capitalism" [ênfase adicionada]

"Judiciário pessoal" é uma ideia que Locke apresenta no *Segundo Tratado do Governo*. O termo refere-se ao direito natural de uma pessoa de avaliar suas próprias experiências e agir de acordo com suas conclusões; isso inclui julgar seu próprio caso. Além disso, como todos têm o

direito de reclamar sua propriedade de um ladrão, todos podem agir como seu próprio agente de restituição. Se alguém roubar sua carteira, você tem o direito de pegar o ladrão para recuperá-la. O agarrar é um ato de força defensiva, não de agressão.

Locke reconhece esse direito, mas acha insensato exercê-lo. Ele escreve:

> Que no estado de natureza cada um tem o poder executivo da lei de natureza, não duvido, mas será objetado que não é razoável que os homens sejam juízes em seus próprios casos, que o amor-próprio torne os homens parciais para si mesmos e seus amigos. E por outro lado, essa má natureza – paixão e vingança – os levará longe demais ao punir os outros; e, portanto, nada além de confusão e desordem se seguirão.

Não é sensato que os homens julguem seus próprios casos porque o ato produzirá conflito na sociedade. Mesmo um homem justo vê as coisas de sua própria perspectiva e interesse próprio; esta é a natureza humana. Além disso, ele pode se enganar sobre os fatos, inclusive fundamentais como a identidade do ladrão. Em outras palavras, mesmo um homem bom carece de objetividade. As pessoas que são menos honestas ou mais emocionais podem ser ainda menos justas e podem exigir remédios inapropriadamente severos.

Locke argumenta que uma sociedade na qual as pessoas julgam seus próprios casos cairá em "confusão e desordem". Por quê? Porque um veredicto injusto ou um remédio impróprio prejudica o destinatário que então julga *seu* próprio caso e retifica o malfeito a ele. O processo pode se tornar um ciclo sem fim porque a justiça administrada não é aceita como legítima por ambas as partes.

Locke acredita que quebrar o ciclo requer um juiz imparcial cuja avaliação seja amplamente aceita como legítima. Em termos de criptografia: Locke quer que a justiça descentralizada de cada homem julgando seu próprio caso seja centralizada e colocada sob a autoridade de uma terceira parte confiável. A necessidade de legitimidade na justiça é uma das principais razões pelas quais Locke defende um estado limitado. E, durante séculos, a abordagem de Locke tem sido usada para argumentar contra a possibilidade de direito privado e justiça na sociedade civil.

Mas se uma terceira parte confiável é irrelevante para exercer direitos como a liberdade de religião, ele não deveria ser verdade para o exercício de uma reivindicação de direito de propriedade sobre bens? Se a criptomoeda for roubada, a vítima não deveria poder recuperar sua propriedade diretamente hackeando as moedas?

Sim, diria Locke, mas há boas razões para não a exercer. Remédios individuais apresentam perigo para a vítima. Primeiro, se ele estiver enganado sobre a identidade do ladrão, o erro converte um ato de legítima defesa em uma agressão pela qual ele é responsável. Em segundo lugar, a vítima pode buscar mais remédios do que o apropriado, levando o agressor original a retaliar. Alcançar a restituição também pode ser perigoso ou além da capacidade da vítima. E assim por diante e assim por diante.

Julgar seu próprio caso também introduz o problema do bom samaritano. Os espectadores basearão seus julgamentos na aparência. Se eles testemunham um ataque na rua desde o início, eles sabem quem é o agressor, é claro. Sabem? E se você testemunhar um homem agarrar uma mulher e puxá-la rudemente para ele? Ela grita por socorro. Você corre para o resgate, atingindo o homem no rosto com um livro pesado que está carregando. Enquanto ele cobre o nariz quebrado, a mulher libertada sai correndo. Mais tarde você descobre que a mulher é uma batedora de carteiras; o homem estava recuperando uma carteira roubada.

Você facilitou um crime e feriu um homem inocente. E, no entanto, tudo o que você pretendia fazer era exercer um princípio corolário de autodefesa: o direito de defender pessoas inocentes contra agressões. Sem esse corolário, os cônjuges não poderiam se defender legitimamente e os pais não poderiam proteger os filhos. Você se comportou de maneira razoável, mas sua avaliação foi incorreta. O homem tinha o direito de cobrar remediação dela, e agora de você.

A confusão pode ser maior com o roubo de criptomoedas. Considere um cenário. Sua conta em uma corretora ou em seu disco rígido é limpa de moedas. Através do trabalho de detetive, você identifica o ladrão e busca a restituição invadindo sua carteira. Sua corretora detecta a atividade e vê *você* como o criminoso simplesmente porque é assim que aparece. A corretora chama a polícia e processa você. Eventualmente, você limpa seu nome à custa de dinheiro, inconveniência e constrangimento. Além disso, você não recupera as moedas.

Muitas vezes é impossível para um espectador distinguir entre uma vítima e um agressor através da observação. Isso é especialmente verdadeiro com crimes de criptomoedas. O homem que recupera sua carteira pode provar que é *sua* carteira mostrando o ID interno. Não é igualmente fácil provar que moedas ou dinheiro fiduciário pertencem a uma pessoa – uma moeda é uma moeda, um dólar é um dólar e eles não vêm com certificados de propriedade.

Felizmente, há uma maneira segura de identificar quem é a vítima.

O teste decisivo: quem é o proprietário do imóvel em questão? Ser proprietário significa ter um título válido para a propriedade. A posse pode até ser "9/10 da propriedade", mas o título é 100%. Ainda assim, a prova de título requer uma determinação baseada no exame das evidências.

> Se nenhum homem pode invadir a propriedade "justa" de outra pessoa, qual deve ser nosso critério de justiça? Não há espaço aqui para elaborar uma teoria da justiça nos títulos de propriedade. Basta dizer que o axioma básico da teoria política libertária sustenta que todo homem é dono de si mesmo, tendo jurisdição absoluta sobre seu próprio corpo. […] Segue-se então que cada pessoa é a justa proprietária de quaisquer recursos previamente não reclamados aos quais ela apropria ou mistura seu trabalho". A partir desses axiomas gêmeos – donidade de si mesmo e "apropriação original" – derivam a justificativa para todo o sistema de títulos de direitos de propriedade em uma sociedade de livre mercado. Este sistema estabelece o direito de cada homem à sua própria pessoa, o direito de doação, de legado (e, concomitantemente, o direito de receber o legado ou herança), e o direito de transferência contratual de títulos de propriedade.
> – Murray Rothbard

Como conceitos, roubo e restituição dependem da ideia de títulos de propriedade. Na maioria dos casos, a restituição é melhor feita por um agente ou agência terceirizada confiável. Contanto que o terceiro seja de livre mercado, isso apresenta poucos problemas. Ao contrário

da aplicação da lei, uma agência de livre mercado pode ser contratada e demitida à vontade. Essa é a diferença entre o Estado e a sociedade.

Antes de prosseguir para uma discussão mais concreta sobre segurança de livre e sua relevância para a criptomoeda, outro aspecto da segurança de livre mercado é melhor abordado: a prevenção do crime.

Segurança preventiva

> Talvez o principal problema nessa área seja ver a importância da proteção – fazer com que as pessoas se concentrem mais em deixar o criminoso fora e menos em prendê-lo depois que ele cometeu um crime. Esforços bem-sucedidos para reduzir a incidência de crimes devem ser baseados em melhores métodos de proteção. Ou seja, devemos nos preocupar em tentar prevenir as transgressões ao invés de nos preocuparmos com o que faremos depois que formos ofendidos. […] Os homens que veem a necessidade de proteção percebem que o governo não está em condições de fornecê-la, e eles dão as costas. A melhor fonte de proteção é o mercado.
> – Robert LeFevre, *The Fundamentals of Liberty*

Uma desvantagem de confiar sua segurança ao estado é a tendência de se tornar dependente dele e negligenciar a proteção a si mesmo. Se não houvesse polícia, as pessoas seriam mais agressivas em garantir preventivamente sua própria segurança. A situação se assemelha a como as pessoas abordam suas contas bancárias. Como a Federal Deposit Insurance Corporation assegura depósitos nos EUA contra falências bancárias, os clientes raramente pensam duas vezes na segurança de suas contas. Essa atitude ou hábito torna as pessoas vulneráveis a perder criptomoedas em corretoras ou investimentos imprudentes. A dependência do estado faz com que percam ou nunca desenvolvam o hábito da autoproteção. No entanto, a autoproteção é tanto responsabilidade do indivíduo quanto sua saúde.

LeFevre destaca outra desvantagem. Aqueles que utilizam os serviços de imposição da lei estão reforçando o mito da legitimidade do estado.

Então, como obter a justiça? LeFevre responde: defesas preventivas que evitam o crime antes que ele aconteça. Isso contrasta fortemente

com a forma como a maioria dos teóricos libertários aborda a justiça privada; eles se concentram quase inteiramente em questões como restituição versus retribuição. Essas questões entram em jogo, no entanto, somente após a ocorrência de uma violação de direitos. Como Satoshi, LeFevre quer um sistema que impeça que os crimes aconteçam em primeiro lugar.

Existem paralelos impressionantes entre LeFevre e Satoshi. Ambos querem evitar e substituir uma agência estatal terceirizada confiável por uma alternativa privada. LeFevre se concentra em substituir a aplicação da lei tradicional, enquanto Satoshi tem como alvo o sistema bancário central. Suas motivações são semelhantes. LeFevre vê a aplicação da lei como um fracasso maciço, ou muito pior. Sob o pretexto de fornecer justiça, oprime os indivíduos regulando quase todas as atividades deixando-os sem fôlego. Da mesma forma, Satoshi sabe que os bancos centrais e o dinheiro fiduciário são fracassos maciços, ou muito piores. Sob o pretexto de fornecer estabilidade e proteção financeira, eles saqueiam a riqueza dos indivíduos por meio de mecanismos como a inflação.

Ambos os homens não enfrentaram o estado, mas evitaram a necessidade dele. LeFevre escreve: “O governo é o único dispositivo que conhecemos de autoproteção? Não, não é. O seguro voluntário é outro dispositivo. Assim como policiais particulares, organizações privadas como a Legião Americana, vigias noturnos, polícia mercante, a Triple A e talvez uma dúzia de outros…”

As vantagens práticas aderem ao compromisso de LeFevre e Satoshi com a prevenção. Por um lado, após a ocorrência de um crime, pode ser quase impossível remediar a vítima, mesmo em casos não criminais de contrato ou atos ilícitos simples.

O estado não quer que as pessoas se protejam a si mesmas porque isso quebra seus monopólios de terceiras partes confiáveis sobre a aplicação da lei e os bancos. Ou, pelo menos, os ignora. O estado quer que as pessoas acreditem que a polícia “serve e protege”, porque então eles aceitam a perda da liberdade como o preço da segurança. A principal arma de autodefesa da sociedade é demonstrar que a proteção e os serviços do estado são desnecessários. As pessoas não precisam pagar com sua liberdade para estarem seguras

Uma Pergunta Assombrosa

A ênfase na prevenção captura um cisma dentro da comunidade cripto. Prevenção e desvio são companheiros naturais. O confronto não é. Qual abordagem é mais eficaz para lidar com o estado? Ou será que pode mesmo ser feita uma declaração geral? Satoshi parecia favorecer a ênfase na prevenção.

As duas atitudes estão incorporadas em um incidente entre Julian Assange e Satoshi. Ambos entendem completamente o valor da liberdade de cripto, mas parecem discordar sobre a melhor maneira de alcançá-lo.

Assange twittou em outubro de 2017: "Meus mais profundos agradecimentos ao governo dos EUA, senador McCain e senador Lieberman por pressionar Visa, MasterCad [sic], Paypal, AmEx, Moneybookers, e outros, a erguer um bloqueio bancário ilegal contra @WikiLeaks começando em 2010. Isso nos levou a investir em Bitcoin – com retornos > 50.000%.

A atitude de Satoshi é sintetizada por sua resposta a um tweet anterior de Assange que declara: "Pode vir [bitcoin]". Objetou Satoshi: "Não, não 'faça isso'. O projeto precisa crescer gradualmente para que o software possa ser fortalecido ao longo do caminho. Faço este apelo ao WikiLeaks para não tentar usar o Bitcoin. Bitcoin é uma pequena comunidade beta em sua infância." Menos de uma semana depois, em 12 de dezembro de 2010, Satoshi desapareceu após postar a mensagem: "WikiLeaks chutou o ninho de vespas, e o enxame está vindo em nossa direção". O enxame é o governo e, talvez, aqueles usuários que não se importam com o Bitcoin como veículo de liberdade e podem diluir seu potencial.

É tentador especular sobre o software com o qual Satoshi queria fortalecer o Bitcoin. Proteções contra maus agentes? Uma corretora descentralizada para negociação complexa e saque? É perturbador perceber que o Bitcoin pode ter sido prejudicado ao se popularizar cedo demais.

Mas a principal questão colocada aqui é se a atitude de prevenção e evasão de Satoshi é a abordagem mais eficaz para combater o estado. Nesse caso, aqueles que confrontam o estado com provocações e desafios podem estar enfraquecendo uma força primária da criptomoeda: liberdade por meio da prevenção, não do confronto. Eles podem estar devolvendo uma vantagem ao estado e afastando-a da sociedade. As teorias e estratégias de resistência não-violenta oferecem um plano de como lidar com o estado.

SEÇÃO CINCO

Cripto, Lei e Justiça

CAPÍTULO ONZE

Lidando com o Crime sem o Estado

O desafio último para a cripto é o mesmo que confronta o próprio anarquismo: e enquanto a lei e a ordem? Como pode o crime ser prevenido e corrigido?

Os seres humanos precisam de justiça tão certamente quanto eles precisam de comida e abrigo. É um bem econômico que o livre mercado pode e irá satisfazer para lucrar. A dinâmica de como as criptos podem prevenir e corrigir o crime será amplamente tecnológica. Elas irão evoluir constantemente para atender às circunstâncias e preferências, a maioria das quais são imprevisíveis. O propósito aqui é esboçar os princípios e o contexto dentro do qual a justiça do livre mercado precisa funcionar e argumentar a favor de sua superioridade sobre o sistema estatal.

Comparado ao que?

A perfeição não existe. Ao avaliar e comparar sistemas que supostamente abordam o mesmo problema, pelo menos duas perguntas devem ser respondidas. Qual é o objetivo de cada sistema? E com que eficácia conseguem atingi-lo?

Apesar da palavra "justiça" aparecer em ambos os termos, os objetivos da justiça do livre mercado e da justiça do estado são incompatíveis. Uma empodera o indivíduo; a outra centraliza o poder nas mãos da autoridade. A justiça de livre mercado é a plena realização do direito de um indivíduo à autodefesa; a justiça estatal destrói o direito de autodefesa ao centralizá-lo nas mãos da autoridade. A situação é semelhante à do domínio financeiro. As criptomoedas e as blockchains permitem que os indivíduos se tornem self-bankers e controlem suas próprias finanças; moeda fiduciária e bancos centrais permitem que o estado monopolize as finanças e tire o controle das mãos dos indivíduos.

A metodologia e os objetivos dos dois sistemas são diametralmente opostos e, para compreendê-los, é útil compará-los especialmente no que diz respeito aos crimes cometidos por indivíduos uns contra os outros.

No entanto, deve-se primeiro declarar uma vantagem fundamental da justiça de livre mercado. A justiça de livre mercado aborda apenas o problema do crime – isto é, a violação de direitos – e atua apenas para

remediar as vítimas. O estado cria pseudocrimes – isto é, criminaliza o comportamento que é pacífico, porém "ofensivo" – e age apenas para proteger seu próprio poder. É difícil exagerar o impacto dessa diferença.

> O governo é uma fábrica de leis. Aprova leis da mesma maneira que uma fábrica produz e vende peças de metal [...], Mas, enquanto a fábrica está fornecendo um produto que é útil para os cidadãos em geral, e que os cidadãos que as comprarem o farão voluntariamente, a fábrica governamental fornece a coerção, que é útil principalmente para o próprio governo, e essa coerção é "comprada" [através de impostos e outras 'taxas'] antecipadamente pelo povo, que nunca está em posição de recusar a "compra".
> – Robert LeFevre, *The Nature of Man and It's Government*.

O sistema de justiça do estado fabrica rotineiramente dois tipos de criminosos reais – pessoas que violam intencionalmente os direitos dos outros. O maior grupo é formado por criminosos santificados que saqueiam riquezas e impõem o controle social em nome do estado. São políticos, burocratas, agentes da lei e outros agentes do estado ou seus comparsas. Quando as pessoas aceitam sua alegação de legitimidade e obedecem, eles governam com luvas de veludo. No entanto, quando as pessoas se recusam, a verdadeira natureza do sistema se revela e a obediência é comandada por meio da coerção crua: a violência.

O segundo grupo consiste em criminosos não santificados. São indivíduos que escolhem a violência ou a ameaça dela como um caminho rápido para o lucro, mas o fazem sem a pretensão de legitimidade. Criminosos comuns existiriam em qualquer sistema, mas a justiça estatal multiplica seu número oprimindo as pessoas de maneira a arrancar delas sua humanidade e a fazê-las abandonar toda crença na lei – qualquer lei. As prisões atuam como campos de treinamento para o crime; não apenas no sentido prático – o de como fazer –, mas também no sentido psicológico: o de por que fazer.

O sistema também produz pseudocriminosos – isto é, pessoas cujo comportamento é pacífico, porém "ofensivo", isto é: inaceitável para o estado. Traficantes e usuários de drogas são exemplos.

O estado se beneficia da fabricação de criminosos de pelo menos quatro maneiras:

- A necessidade humana de segurança e justiça dá ao estado uma justificativa para reivindicar o monopólio do uso da violência. O estado então centraliza e industrializa os "serviços" que fornece: a indústria legislativa, as burocracias regulatórias, a indústria policial, o sistema judiciário, a indústria prisional, o estado de vigilância e uma infinidade de outras indústrias associadas. O poder do estado está cimentado em todos os nichos da vida cotidiana.
- Se as pessoas acreditam que o estado é a única fonte de segurança, elas aceitam de bom grado a violência cometida por seus agentes. O povo presta obediência em troca de proteção, crendo não haver alternativa.
- O estado justifica impostos, multas e outras taxas em nome do financiamento da lei e da ordem. A "segurança" e todos os seus custos de fabricação, aplicação e manutenção são as gansas dos ovos de ouro dessa organização.
- Dinâmicas menos diretas, como o trabalho prisional, são extremamente lucrativas para o estado e para seus cúmplices corporativistas, que usam as prisões como centros fabris com mão de obra extraordinariamente barata.

Uma abordagem totalmente diferente é necessária para preencher a necessidade humana de segurança e justiça. Nada atende às necessidades humanas de forma tão eficiente e imparcial quanto o livre mercado. É necessário um retorno às raízes.

As apostas são altas. Reconsidere aquilo que atualmente dizem ser justiça.

O estado destrói o que não pode controlar

Comparar a justiça do livre mercado e a justiça estatal requer uma compreensão dos objetivos e da metodologia de cada uma. A justiça de livre mercado procura proteger a pessoa e a propriedade dos indivíduos e retificar qualquer violação com o mínimo de força possível. A justiça estatal busca manter o controle do estado sobre a sociedade e punir qualquer violação de suas regras com a força necessária para desencorajar novas violações. O objetivo do estado faz dele uma fábrica de leis; sua metodologia o torna uma fábrica de crimes.

> A maioria das pessoas não consegue avaliar os obstáculos fundamentais colocados no caminho da prevenção do crime pela lógica perversa da propriedade *pública*, da aplicação da lei *pública* e da prisão *pública*. Primeiro passo: comece com ruas públicas, calçadas e parques onde todos os cidadãos devem ter permissão de uso, a menos que se provem culpados de um crime. Etapa dois: apoie-se sobre uma burocracia pública inerentemente ineficiente para capturar, processar e julgar os criminosos contra os quais existem evidências suficientes de culpa. Terceiro passo: caso sejam condenados, sujeite os criminosos a um ambiente perigoso, improdutivo e, às vezes, incontrolável das prisões públicas para impedi-los de cometer futuras conduta antissociais. Etapa quatro: libere periodicamente a maioria dos prisioneiros de volta à sociedade e, depois, retorne à etapa um e repita o ciclo indefinidamente. Cada passo segue o passo anterior, e cada passo inevitavelmente deixa um espaço considerável para a conduta criminosa prosperar.
> – Randy Barnett, *The Structure of Liberty: Justice and the Rule of Law*.

Em suma, o estado cria criminosos não apenas por meio da legislação, mas também através de seu método de punição. Ele reivindica autoridade sobre o próprio cimento que as pessoas pisam, e depois as criminaliza por qualquer passo em falso. Isso não ajuda vítimas reais. Uma vez dentro do sistema de justiça, os criminosos têm pouca ou nenhuma chance de remediar seus erros por meio da restituição. Para a justiça estatal, a vítima geralmente é o próprio estado. Isso é especialmente verdadeiro para crimes sem vítimas – os chamados "crimes", nos quais todos os envolvidos, ironicamente, participam voluntariamente. Os crimes sem vítimas são responsáveis pela maioria das prisões.

O monopólio estatal da força é essencial para manter todos os outros monopólios, inclusive sobre o fluxo financeiro. Qualquer pessoa ou qualquer coisa que ameace esses monopólios é criminalizada, incluindo as criptomoedas. O estado identifica com precisão as criptomoedas como uma violação de seu monopólio e privilégios monetários. Isso significa que contornar o estado e os bancos centrais é criminalizado por estar associado à atividade do mercado negro e a outras condutas

pacíficas que privam o estado de receita. Esses pseudocrimes "justificam" a repressão estatal. Claro, as pessoas que usam dinheiro fazem o mesmo, mas há uma diferença notável na forma como o estado lida com crimes financeiros:

1. Os usuários-alvo são demonizados – profissionais do sexo, por exemplo – mas o dinheiro em si não é acusado de ser criminoso, talvez porque seja emitido por um agente do estado. Ou seja, a grande maioria das pessoas que usam dinheiro não são vistas como meliantes. Por outro lado, *tanto* os usuários *quanto* as criptos são demonizadas. A cripto é o verdadeiro alvo, com categorias de usuários que são vistas como desagradáveis sendo atacadas com destaque; uma tentativa de minar a legitimidade das criptomoedas.
2. Toda a categoria de usuários de criptomoedas é criminalizada – ou melhor, toda a categoria daqueles que usam criptomoedas *não regulamentadas*. Esta é uma característica da justiça estatal. Categorias de pessoas se tornam criminosas – traficantes de drogas e profissionais do sexo, por exemplo – independentemente de algum deles ter agredido outro indivíduo. Novamente, o dinheiro está isento desse tratamento, com a grande maioria dos que usam o dinheiro estatal não sendo acusados de crime.

O problema fundamental do estado com as criptomoedas, em oposição ao dinheiro, é que as criptomoedas tornam possível confiar em estranhos. Isso faz do próprio estado um estranho, porque ele é sempre o último a ser confiável. Se os indivíduos não exigirem os serviços do estado, não haverá razão legítima para ele existir. É por isso que o estado está tão desesperado para convencer as pessoas de que elas precisam dele para ter dinheiro, segurança, aposentadoria, assistência médica, educação e todos os outros bens do livre mercado e todos os outros serviços que puderem requisitar. O atual sistema de justiça não trata da proteção da sociedade ou dos indivíduos, mas da preservação do estado.

Infelizmente, uma segunda justificativa apoia a campanha do estado contra as criptomoedas não regulamentadas: a alegação de que as criptomoedas violam os direitos individuais. Especificamente, diz-se que as criptomoedas estão envolvidas em violência contra indivíduos, como o tráfico humano. O aspecto "infeliz" dessa justificativa é que algumas acusações são verdadeiras. Este é o ataque mais perigoso do estado às criptomoedas, porque dá a entender que pessoas decentes que

ficam e devem ficar horrorizadas com crimes como o tráfico humano simpatizam com ele.

Um artigo do bitcoin.com de março de 2018 aborda outro crime real: fraude. "Todos os dias são perdidos cerca de $9 milhões em golpes de criptomoedas."

> No tempo que você leva para ler esta frase, $850 terão sido perdidos em golpes de criptomoeda. No tempo necessário para concluir este artigo, esse valor terá subido para $17.000. Phishing; fraude; roubo; hacking; e os números são sempre altos. Nos primeiros dois meses de 2018, ocorreram 22 golpes separados envolvendo roubos de $400.000 ou mais. Junte todos os números e isso equivale a uma média de $9,1 milhões por dia. Ah, e isso não inclui os valores discrepantes de 2018 – Coincheck, Bitconnect e Bitgrail. Caso contrário, o total seria de $23 milhões por dia.

O estado usa crimes reais como cobertura para atingir seu verdadeiro objetivo em relação à cripto: eliminar a concorrência que ameaça um de seus monopólios vitais: o dinheiro. Parte da campanha do estado é exagerar os crimes reais, e com isso apresentar seu serviço como o único remédio possível.

As criptomoedas são acusadas de proteger quase todos os atos de violência concebíveis. O artigo "10 das maiores mentiras contadas sobre o Bitcoin" trata da acusação de que as criptomoedas são o dinheiro preferido do terrorismo.

> Se você quer culpar uma moeda, tente o dólar americano, que tem sido usado para financiar mais guerras, guerras por procuração, bombardeios, sequestros e insurgências do que qualquer outra moeda. A Europol não encontrou evidências de que terroristas estivessem usando criptomoedas para financiar suas atividades. Isso não quer dizer que já não tenha acontecido ou que não vá acontecer. É revelador, no entanto, que as únicas pessoas que ligam o bitcoin ao terrorismo são os governos, que buscam reprimir as moedas digitais.

As criptos também são acusadas de facilitar grupos de ódio.

> Poderíamos lançar uma longa explicação sobre o porquê de ser ridículo culpar uma moeda pelas ações de um pequeno subconjunto de seus usuários, mas às vezes as respostas mais simples são as melhores: “Você provavelmente já ouviu falar sobre carros – mas o que você certamente não ouviu é o quanto eles estão ajudando os ladrões de banco.”

Muitas vezes é difícil enxergar através da fumaça, discernir os crimes frios e cruéis nos quais as criptomoedas estão envolvidas das próprias criptomoedas. Mesmo assim, esses crimes devem ser combatidos. E não apenas porque convidam ao envolvimento do Estado, mas também porque as vítimas merecem reparação. No entanto, concordar com o Estado neste ponto é o início de uma disputa mais profunda que se resume a questões mais fundamentais.

O que é Justiça?

> O libertarianismo é sobre direitos individuais, direitos de propriedade, livre mercado, capitalismo, justiça ou o princípio de não agressão. Ainda assim, nenhuma dessas coisas é suficiente para explicá-lo completamente. O capitalismo e o livre mercado descrevem as condições catalácticas que surgem ou são permitidas em uma sociedade libertária, mas não abrangem outros aspectos do libertarianismo. E direitos individuais, justiça e agressão resultam em direitos de propriedade, pois, como Murray Rothbard explicou, direitos individuais são direitos de propriedade. E a justiça é apenas dar a alguém o que lhe é devido, e isso depende de quais são seus direitos.
> – Stephan Kinsella, “What Libertarianism Is.”

O que é justiça? A resposta é: a estrutura rudimentar de qualquer sistema de direito. O filósofo político americano Michael Sandel responde: “A maneira mais simples de entender a justiça é dar às pessoas o que elas merecem. Essa ideia remonta a Aristóteles. A verdadeira dificuldade começa com descobrir *quem* merece *o quê* e *o porquê*”. [Ênfase adicionada] Isso é justiça privada. Ela precisa de mais definição.

A justiça privada é distinta da justiça divina, mas às vezes as duas se confundem. A justiça divina supõe uma deidade ou algum outro poder supremo responsável e capaz de pesar o valor de cada pessoa em uma balança, aplicando ao réu o destino que a deidade julgar como justo. "Por que eu, ó Senhor, por que eu?" é o grito de quem acredita ter sido traído pela justiça divina. A teoria por trás desse "grito de socorro" é que há algo, além da não agressão contra sua propriedade, que uma boa pessoa tem o direito de exigir do mundo: boa saúde, por exemplo. Quando coisas ruins acontecem, a situação é chamada de "injusta". Porém, a palavra está sendo usada coloquialmente ou sendo mal utilizada. Talvez uma palavra melhor seria "azar".

A justiça privada não é baseada em uma divindade ou algum outro poder transcendente. É, como sustenta Aristóteles, justiça que consiste nas pessoas receberem o que merecem umas das outras. E, como Kinsella explica na primeira citação: "justiça é apenas dar a alguém o que lhe é devido, e isso depende de quais são seus direitos". Baseia-se na natureza humana e na autopropriedade de cada indivíduo.

O conteúdo da justiça privada baseia-se em dois princípios. A primeira é a não iniciação da força, que é uma reafirmação do dever de uma pessoa de respeitar a autopropriedade dos outros; a justiça reside em viver juntos em paz. O segundo princípio é o direito contratual, pelo qual uma pessoa troca voluntariamente com outra. A justiça aqui reside em cada pessoa recebendo o que foi acordado. Quando a justiça não ocorre, é necessário um remédio. No entanto, nem uma quebra de contrato nem seu remédio precisam envolver violência. Uma violação nem sequer precisa ser culpa de uma pessoa; poderia ser ocasionada por qualquer outra coisa, como uma mudança inesperada das circunstâncias. Mesmo assim, a pessoa prejudicada pela violação ainda tem o direito de ser remediada.

É aí que começa e termina o direito à justiça. Porém, há uma confusão comum sobre justiça. Nominalmente, muitas vezes é chamado de "injusto" quando uma parte trata a outra com desrespeito ou hostilidade. Isso pressupõe que uma pessoa possa ter, numa situação dessas, o direito à reivindicação de reparação pela atitude da outra pessoa. Mas, esse direito não existe; há apenas o direito de viver sem ser agredido ou ameaçado e ao cumprimento de um contrato. É improvável que um vendedor que seja rude com um comprador tenha negócios repetidos, e isso é um forte incentivo para que ele seja civilizado. Mas o único dever do vendedor sob a justiça é ser não violento e ser honesto na troca; ser

agradável, embora favorável a ambas as partes, é totalmente opcional. Como Rothbard escreve: “Não é função da lei tornar alguém bom, reverente, moral, educado ou gentil”.

Voltando à declaração inicial de Sandel, o *quem* da justiça é duplo: 1) quem é privado do que é seu por direito – autonomia corporal, propriedade ou um benefício contratado, 2) e quem é responsável por fornecer reparação à vítima. O *como* é abordado neste capítulo. O *porquê* é por conta do fato de cada pessoa ser um proprietário de si mesmo.

Poucas coisas são tão justas quanto o livre mercado, em que duas pessoas trocam diretamente por valores acordados e depois vão embora, cada uma satisfeita. Uma mulher que compra um tomate e vai para casa com sua compra para fazer uma salada está aproveitando a justiça. O vendedor de tomates que embolsa o dinheiro da mulher e passa para o próximo cliente também está experenciando a justiça. Assim, o livre mercado oferece às pessoas o que elas merecem por direito. Em outras palavras: o livre mercado é a justiça aristotélica na prática.

Outra maneira de dizer isso é que a justiça privada é proprietária. Em seu ensaio “A Teoria Proprietária da Justiça na Tradição Libertária”, o cofundador do Movimento Voluntarista Moderno, Carl Watner, fornece um resumo justo da justiça privada: “A teoria proprietária da justiça está preocupada com apenas uma coisa: a determinação crucial de títulos de propriedade justos versus títulos de propriedade injustos de indivíduos em relação a seus próprios corpos e aos objetos materiais ao seu redor.”

O teórico mais persuasivo da justiça proprietária pode muito bem ser o jurista libertário Randy Barnett. Em seu livro *The Structure of Liberty*, Barnett argumenta que a lei deve ser administrada de forma privada, com quaisquer ineficiências deixadas sob a responsabilidade do livre mercado. Parte da eficiência da justiça proprietária deriva de sua pura simplicidade e do número mínimo de leis. Barnett escreve sobre o sistema atual: “Cada dólar gasto para punir um usuário ou vendedor de drogas é um dólar que não pode ser gasto cobrando restituição de um ladrão. Cada hora gasta investigando um usuário ou vendedor de drogas é uma hora que poderia ter sido usada para encontrar uma criança desaparecida. Todo julgamento realizado para processar um usuário ou vendedor de drogas é tempo de tribunal que pode ser usado para processar um estuprador”. Barnett argumenta que o direito privado é a solução para a corrupção inevitável que surge dos interesses adquiridos e dos monopólios.

Os Requisitos do Direito de Contratos Privados

O direito contratual exige apenas duas coisas para funcionar: a presença de um acordo e um instrumento de execução. O contrato é a presença do acordo; expressa o consentimento e os termos de aceitação. Os contratos podem ser implícitos, verbais ou escritos, mas quanto mais explícito for o acordo mais fácil será a administração da justiça.

O obstáculo sobre o qual a lei muitas vezes tropeça é o instrumento de execução. Como você aplica a lei em outra pessoa e executa restituição? Surgem daí questões éticas e práticas. Uma questão ética comum: e os direitos individuais daqueles forçados a fornecer restituição? Uma resposta comum: quem viola os direitos de outro renuncia aos seus na proporção do dano infligido e até que esse dano seja remediado. Uma questão prática comum: a restituição convida à participação de uma terceira parte confiável. Na lei estatal, a terceira parte é composta por agentes do estado, que costumam usar a violência. No direito proprietário ou de livre mercado o terceiro consiste em agentes do livre mercado, que são restringidos por dinâmicas como o uso da força proporcional e a necessidade de preservar uma boa reputação. Mas qualquer modelo que dependa de uma terceira parte confiável é vulnerável à corrupção, incompetência e outros riscos.

Satoshi removeu das trocas econômicas o problema das terceiras partes confiáveis, e a blockchain também pode removê-lo de muitas áreas da lei. Uma transferência peer-to-peer na blockchain atende a todos os requisitos de um bom contrato. Ela incorpora um acordo voluntário; memoriza os termos da troca; sua validade é comprovada pela transparência. A blockchain também pode cumprir um dos requisitos da lei – ou seja, é um instrumento de execução por si só. Quando isso acontece, é chamado de contrato inteligente – um contrato autoexecutável. Um relatório recente do Senado dos EUA afirma: “O conceito [de contratos inteligentes] está enraizado no direito básico dos contratos. Normalmente, o sistema judicial julga disputas contratuais e impõe termos. Com os contratos inteligentes, um programa impõe o contrato embutido no próprio código.” Os contratos inteligentes oferecem a mesma oportunidade de evitar terceiras partes confiáveis de advogados e tribunais do estado, assim como as criptomoedas evitam os bancos centrais. Além disso, ao atuar como o acordo e o instrumento de execução, a

criptomoeda pode eliminar grande parte das despesas dos serviços de justiça.

Os contratos inteligentes de hoje são, sem dúvida, primitivos em comparação aos que virão, mas também são uma prova de que a ideia funciona.

O impacto na sociedade causado pela tecnologia dos contratos autoexecutáveis pode ser enorme. Em uma sociedade organizada em torno da troca, os contratos seriam a base de *toda* lei. Até o uso da violência, que viola os direitos individuais, pode ser visto como uma violação do dever – o contrato implícito – de que todos devem respeitar os direitos dos outros se quiserem reivindicar esses direitos para si. Mais uma vez, aqueles que cometem crimes perdem seus próprios direitos na mesma medida em que os negaram a outrem e enquanto o erro não for sanado, isto é: enquanto a vítima não for remediada. Em seguida, o contrato é restabelecido. Toda lei pode ser reduzida ao contrato.

Um artigo no *Futurism*, “Um escritório de advocacia de IA quer automatizar todo o mundo jurídico”, indica o quão fácil pode ser a transição de contratos físicos e advogados para contratos inteligentes e algoritmos. “No LawGeex [um serviço automatizado], os usuários carregam um contrato e, em um curto período (uma hora, em média), recebem um relatório informando quais cláusulas não atendem aos padrões legais comuns. O relatório também detalha quaisquer cláusulas vitais que possam estar faltando e onde cláusulas existentes podem exigir revisão. Tudo isso é calculado por algoritmos.” Por uma taxa modesta, a LawGeex pode detectar cláusulas que permitem fraudes ou fornecem proteção inadequada.

Esses serviços destacam um aspecto raramente discutido da justiça: o fato de que ela é um serviço. Basicamente, há dois aspectos da justiça proprietária: Os proprietários devem pagar o custo de proteger sua propriedade, se assim o desejarem e os criminosos devem pagar todos os custos da restituição, que incluem a própria restituição, as despesas para obter a remediação e a inconveniência ou sofrimento da vítima.

> “A análise econômica do crime começa com uma simples suposição: os criminosos são racionais. Um assaltante é um assaltante […] porque essa profissão o torna melhor, segundo seus próprios padrões, do que qualquer outra alter-

> nativa disponível para ele […] Se os assaltantes são racionais, não temos que tornar o assalto impossível para evitá-lo, apenas inútil … Se velhinhas começarem a carregar pistolas em suas bolsas, de modo que um assalto em dez coloca o assaltante no hospital ou no necrotério, o número de assaltantes diminuirá drasticamente – não porque todos tenham sido baleados, mas porque a maioria terá mudado para formas mais seguras de ganhar a vida. Se o assalto se tornar suficientemente não lucrativo, ninguém o fará".
> – David Friedman, *Rational Criminals and Profit-Maximizing Police*.

Qualquer um que valorize sua propriedade deve tornar os crimes contra ela não lucrativos e difíceis. Essa abordagem por si só poderia reduzir em muito os crimes. No entanto, as pessoas geralmente lidam com sua segurança pessoal de uma dessas quatro formas:

- Elas se auto protegem, assumindo diretamente a responsabilidade por sua própria segurança e pela de sua propriedade. Isso envolve custos como fechaduras, prática de autodefesa e, portanto, um certo investimento de tempo.
- As pessoas ignoram sua própria segurança, confiando na sorte ou na boa vontade dos outros. O custo é o dano potencial à sua propriedade e à sua pessoa.
- As pessoas confiam na proteção do estado. O custo é a sua liberdade e a chance de segurança real.
- As pessoas veem a segurança como um serviço privado ao qual assinam – contratar um vigia noturno, por exemplo. O custo é o custo do serviço.

Se segurança é um bem econômico, como comida ou abrigo, então o consumidor do bem deve arcar com o preço de adquiri-lo, e o custo nem sempre é monetário. O preço a se pagar pode muito bem ser o tempo e a energia necessários para configurar proteções. (Veja a discussão sobre proteção no capítulo anterior).

Um vislumbre de como a proteção do livre mercado pode funcionar para as comunidades são as redes de confiança (networks), que não contam com a proteção da polícia, e que ainda assim precisam cuidar e

cuidam de si mesmas. Considere as profissionais do sexo. A propriedade a ser protegida, nesse caso, é o próprio corpo da profissional do sexo.

Em seu artigo "Cem anos de anarquia criptográfica", a engenheira Blockchain Elaine Ou comenta: "A encriptação de chave pública não serve apenas para encriptar mensagens privadas. Ela também fornece provas de que o remetente é quem diz ser. Quando compradores e vendedores realizam transações, eles assinam mensagens com suas chaves privadas. As assinaturas se tornam identificadores digitais." Se isso parece muito distante da prevenção à violência, converse com profissionais do sexo, cuja principal forma de defesa é verificar as identidades e reputações dos clientes, que elas compartilham umas com as outras por meio de redes de confiança (networks). Uma das responsabilidades menosprezadas de um cafetão – muitos dos quais não são abusivos – é garantir a segurança das profissionais do sexo, seja examinando clientes, manuseando dinheiro, fornecendo transporte ou lugares seguros e esperando. Os cafetões são terceiras partes confiáveis, mas como quaisquer terceiros, podem trazer mais problemas do que soluções. A criptografia muda essa dinâmica para que algumas tarefas de um cafetão sejam substituídas por um filtro peer-to-peer com transparência. Assim, a profissional do sexo está no controle, e isso se traduz em menos risco de violência e mais dinheiro, o que promove a segurança.

O segundo aspecto da justiça proprietária é a necessidade de obrigar os criminosos a pagarem o preço de remediação de suas vítimas. Mas como isso poderia se dar?

Um mecanismo de restituição comumente proposto tem sido a agência de defesa privada (PDA). O PDA é um negócio de livre mercado cujos lucros e a reputação dependem da precisão e justiça de suas práticas na remediação do crime. Uma vítima de crime escolhe livremente sua terceira parte confiável, cuja confiança é testada pela presença constante de concorrentes. A relação comercial dura apenas enquanto o cliente valoriza o serviço.

O objetivo do PDA é recuperar das mãos do criminoso os bens roubados ou danificados, ou no mínimo o valor deles; novamente, a propriedade danificada pode ser o corpo da vítima. Mas o PDA também atua como proteção para a vítima e para o próprio agressor durante o processo de remediação. A vítima é protegida de qualquer dano ou perigo que possa estar envolvido; o agressor lida com um profissional que deseja apenas garantir a remediação, e não a dar vazão à raiva da vítima,

de quaisquer outros ou de sua própria. De fato, o PDA tem um forte incentivo comercial para evitar as despesas e complicações de ferir alguém.

Friedman oferece uma visão de um PDA em seu livro *Machinery of Freedom*. De início, o autor considera "o caso mais fácil" de um conflito, que é "a resolução de disputas envolvendo contratos entre firmas bem estabelecidas [...]. Um desenvolvimento recente; historicamente, a aplicação veio do desejo de uma empresa de manter sua reputação".

Mas e as disputas envolvendo violência, incluindo roubo? "A proteção contra a coerção é um serviço", explica Friedman. "Atualmente, é vendido em uma variedade de formas, como guardas da Brinks, fechaduras, alarmes contra roubo etc. À medida que a eficácia da polícia estatal diminui, esses substitutos de mercado para a polícia, como os substitutos de mercado para os tribunais (os contratos inteligentes), tornam-se mais populares. Suponha então que em algum momento futuro não haja polícia estatal, mas sim agências de proteção privada. Essas agências vendem o serviço de proteção a seus clientes. Talvez eles também garantam desempenho ao segurar seus clientes contra perdas resultantes de atos criminosos". O seguro que foi adquirido de um PDA torna-se a solução imediata oferecida à vítima, talvez da mesma maneira que o seguro de carro paga por danos após um acidente; o PDA pode então buscar a solução do criminoso com o bônus de adquirir seu lucro. Ou a vítima pode contratar o PDA após o crime ter sido cometido, e então o PDA investigaria e recuperaria tanto a propriedade quanto o custo de seus serviços diretamente do agressor.

Friedman conclui: "O que descrevi é um arranjo muito improvisado. Na prática, uma vez que as instituições anarcocapitalistas estiverem bem estabelecidas, as agências de proteção antecipariam tais dificuldades e providenciariam contratos com antecedência, antes mesmo que os conflitos específicos ocorressem [...]" Mas, novamente, não é possível prever futuros mecanismos de restituição.

Na verdade, a resposta mais precisa para uma pergunta feita anteriormente – como seria a justiça proprietária? – é uma que muitas pessoas acharão insatisfatória. Ninguém sabe, assim como ninguém sabia como o Bitcoin se formaria e como se manifestaria.

A razão pela qual a aparência futura da justiça proprietária é imprevisível

Na obra *Human Action,* de Ludwig von Mises, onde o autor defende o conceito de "consumidor soberano", que expressa como consumidores e produtores se relacionam em uma economia de mercado. Os produtores são o motor da prosperidade, afirma Mises, mas não são eles que determinam a direção que uma economia toma. Esse poder pertence aos consumidores. Mais especificamente à preferência dos consumidores. Essas preferências diversas levam a uma explosão de escolhas econômicas – uma dinâmica que seria verdadeira para os serviços de segurança e justiça.

A soberania do consumidor vai contra a crença dominante de que são os capitalistas e os grandes empresários que determinam o curso de uma economia, assim como a vida das pessoas, que participam dela. É aquela velha ideia tradicional: a de que o controle econômico está nas mãos de quem tem a propriedade dos meios de produção, enquanto as pessoas comuns são forçadas a aceitar as migalhas.

Para Mises, a relação é simbiótica, sendo o consumidor um parceiro igual ou maior. Ele descreve a soberania do consumidor:

> A direção de todos os assuntos econômicos é, na sociedade de mercado, uma tarefa dos empresários; deles é o controle da produção. Eles estão no leme e dirigem o navio. Um observador superficial acreditaria que eles são supremos. Mas eles não são. Os empresários, ao contrário do que se pode pensar, são obrigados a obedecer incondicionalmente às ordens do capitão, e o capitão é o consumidor. Nem os empresários, nem os agricultores, nem os capitalistas determinam o que deve ser produzido. Apenas os consumidores têm o poder de fazer isso. Se um empresário não obedecer estritamente às ordens do público que lhe são transmitidas pela estrutura de preços de mercado, ele sofre perdas, vai à falência e, assim, é afastado de sua posição no leme. Outros que se saírem melhor em satisfazer a demanda dos consumidores o substituirão.

Uma consequência da soberania do consumidor é que ninguém pode prever as preferências expressas no mercado, incluindo os próprios consumidores. Ninguém pode prever as instituições, agências ou dinâmicas que surgirão para lucrar com essas preferências. Sem dúvida,

a tecnologia e outras inovações evoluirão para oferecer novas alternativas; a mudança será vertiginosa. Mises observa:

> "Eles [os consumidores] não são chefes fáceis. Estão sempre cheios de caprichos e fantasias, mutáveis e imprevisíveis. E não se importam nem um pouco com o mérito passado. Assim que lhes é oferecido algo que eles gostam mais ou é mais barato, os consumidores abandonam seus antigos fornecedores."

O livre mercado muda constantemente em resposta à forma como os consumidores votam com seu dinheiro. É fluido, constante e está além da capacidade de previsão de qualquer pessoa. A soberania do consumidor é uma das principais razões pelas quais não é possível oferecer um plano fixo de como a justiça proprietária funcionará no futuro. Só é possível descrever os conceitos que cercam a justiça, mas não suas aplicações específicas.

Rumo a uma nova visão de justiça

As criptomoedas mudaram a visão do mundo sobre o dinheiro – do que era e do que poderia ser… Ou será. A justiça proprietária também revoluciona o conceito e a aplicação da lei. Em ambos os casos, os princípios e definições permanecem inalterados. O dinheiro é um meio de troca, uma forma de riqueza e uma unidade financeira. Justiça é cada um receber o que merece; a lei é o meio e as regras de execução da justiça. Mas a forma que a justiça proprietária assume, como as criptomoedas, é algo novo sob o sol.

Tradicionalmente, o estado justifica seu monopólio sobre o dinheiro e a justiça apontando para uma suposta necessidade de "consenso". O estado justifica seu monopólio monetário pela chamada necessidade de que uma moeda seja "confiável" e amplamente aceita em um determinado território. Lockeanos justificam o próprio estado pela suposta necessidade da sociedade civil de um árbitro final de justiça cujo julgamento seja "confiável" e geralmente aceito dentro de um determinado território. (O consenso que é compelido pela força, é claro, não é consenso; indica o contrário.)

O consenso é o raciocínio do século passado. É inválido para a moeda; é inválido para a justiça. As criptomoedas provaram que o consentimento individual, junto com um instrumento de aplicação – a blockchain –, cria uma moeda válida. Não importa se os usuários individuais constituem uma pequena parcela da população. Como na América colonial, uma infinidade de moedas pode circular para preencher uma variedade de nichos e preferências. E o mesmo acontece com a justiça.

As pessoas que estabelecem contratos entre si podem ter uma visão de justiça diferente da de seus vizinhos ou do público em geral. A primazia dos contratos e o uso da blockchain significam que, desde que a violência seja evitada, não há uma justiça universal. O que for acordado é justo. Quem acredita que cobrar juros é errado, por exemplo, fará empréstimos que não incluem nenhum. Para os capitalistas, o oposto será verdadeiro. Ambos os arranjos são justos, com o conteúdo da justiça sendo definido pelos seus participantes.

O ponto mais importante: os indivíduos contratantes definirão seu próprio padrão de justiça, que pode e irá variar de contrato para contrato dentro da mesma jurisdição. Isso separa a justiça da geografia – dos ditames de uma autoridade que reivindica jurisdição sobre um determinado território – e localiza o conteúdo da justiça dentro dos próprios indivíduos. A justiça é descentralizada até o nível máximo: o do indivíduo.

O estado recorre ao argumento do consenso porque sua jurisdição está inerentemente ligada à geografia. Uma nação é definida geograficamente e um estado é a instituição que reivindica jurisdição sobre uma nação específica, a qual ele tenta manter sob controle através do monopólio do uso legítimo da força. Na realidade, o consenso que o estado alega ter advém de sua própria autoridade, que todos dentro da jurisdição são compelidos, sob ameaça, a honrar. A população deve aceitar a moeda legal, obedecer à lei e obedecer às vontades e aos decretos de seus juízes; ninguém está autorizado a discordar. Ninguém.

Mas o que acontece quando a geografia se torna irrelevante para a lei e a justiça como a transferência de dinheiro é agora? Nesse caso, o estado ainda seria capaz de exercer sua “autoridade”?

As criptomoedas respondem esta pergunta: Cruzando o globo como o vento e não assumindo qualquer nacionalidade, as criptomoedas sobrevoam pontos físicos de engarrafamento, chamados bancos, assim como linhas imaginárias, chamadas fronteiras. A cripto ignora a geografia, assim como ignora o problema das terceiras partes confiáveis. O

estado perde o monopólio do dinheiro e do sistema financeiro, que é sua força vital. Quando a geografia se torna irrelevante, o estado também se torna, pois o estado é uma reivindicação territorial, e as criptomoedas tratam essa questão de maneira peculiar: elas não dão a mínima.

Esta é a Justiça sem fronteiras geográficas. Esta é a justiça das criptos. A justiça que não passa pelo engarrafamento da lei estatal, que impõe aceitação às normas do estado. Essa é a justiça descentralizada, a que expressa apenas as preferências dos indivíduos envolvidos. Essa noção de justiça visa libertar os indivíduos da "justiça" estatal da mesma maneira que as criptomoedas os libertaram do dinheiro fiduciário monopolizado pelo estado.

Infelizmente, a necessidade percebida de consenso faz com que as pessoas acreditem que a justiça de livre mercado é "anárquica" no pior sentido da palavra. Elas não entendem os princípios, o propósito e conteúdo da justiça proprietária. Seu princípio central é o direito de cada indivíduo de viver em paz. Seu propósito é facilitar as trocas voluntárias entre os indivíduos para que cada um receba o que merece; quando não o fazem, então o propósito se torna a restituição. Exceto pela proibição da violência, o conteúdo da justiça seria tão variado quanto as próprias criptomoedas, porque os indivíduos decidiriam o que é exatamente da mesma maneira que decidem o preço adequado de um bem – por meio de um acordo.

Declarado de outra forma: A blockchain atua como o contrato, a lei e o mecanismo de aplicação em um único pacote. Ela incorpora os termos com os quais as partes concordaram, aplica esses termos sem o envolvimento de terceiros e garante que sua aplicação ocorra sem considerar jurisdições geográficas. Assim como a cripto evita o monopólio monetário, a justiça blockchain pode contornar os monopólios de aplicação da lei e justiça do estado.

A confusão das pessoas sobre a lei e a justiça de livre mercado é compreensível porque os conceitos vão contra tudo o que os foi ensinado. O que aprenderam é incorreto; não apenas a teoria, mas também a história.

Em seu artigo, "Por que as Elites Preferem um Sistema Legal Centralizado", o historiador Chris Calton explica como a visão convencional de justiça centralizada foi incorporada. "A motivação para centralizar a autoridade legal foi inteiramente política." Uma função vital da sociedade civil foi usurpada e homogeneizada em nome da consistência e do consenso. Isto nem sempre foi desse jeito. Calton continua:

> "Mas no início do século XIX, a consistência era menos valorizada do que a flexibilidade no sistema jurídico. Quando os tribunais eram locais, as pessoas de uma determinada comunidade tinham interesse em que a justiça fosse feita de acordo com as particularidades de cada caso individual. [...] E para aqueles que não tiveram a sorte de se encontrar no topo da hierarquia jurídica – os sem instrução, os pobres, as mulheres, as crianças e os negros – essa flexibilidade sustentava até mesmo as noções modernas de justiça – ainda que imperfeitamente – com mais eficácia do que os tribunais centralizados e legalmente consistentes que se seguiram."

A lei foi descentralizada para o nível local, a fim de atender às necessidades da população local. E se a lei centralizada nem sempre existiu, então ela não é inevitável nem necessária. O passo final, é claro, é descentralizar a justiça para o indivíduo.

Na verdade, instâncias de lei descentralizada funcionam ao nosso redor agora e oferecem modelos práticos para a construção de novos sistemas. Uma delas é chamada Creative Commons Law (CCL). A CCL é um empreendimento de código aberto para construir um sistema jurídico prático para sociedades sem estado. Ela enfatiza a aplicação concreta e de forma alguma bloqueia outros sistemas concorrentes. A maioria das pessoas encontrou uma manifestação do CCL: as licenças Creative Commons para publicação de material têm sido tradicionalmente vistas como o limite da propriedade intelectual, dos direitos autorais e patentes.

Muitos autores e inventores descartam a legitimidade da PI e oferecem seu trabalho sem as restrições normais de direitos autorais na republicação; outras licenças Creative Commons especificam termos como creditar a fonte original na reimpressão. O autor ou inventor escolhe a licença que prefere; sua escolha de forma alguma infringe as pessoas que escolhem diferentes termos de publicação, como os que buscam preservar um quase monopólio de seu trabalho. Ideias e desenvolvimento de código aberto têm sido a base da comunidade de cripto. A CCL é uma prova da lei de livre mercado.

Em resumo, a justiça da blockchain é uma justiça proprietária, que está livre das jurisdições geográficas conhecidas como nações. Ela

é limitada, em vez disso, por algoritmos e escolhas. Não requer consenso ou o envolvimento da terceira parte confiável chamado estado. O código é a lei, e o conteúdo do código é o que os envolvidos concordam. Os indivíduos definem e executam sua própria lei sem uma legislatura ou um processo político. E, se a justiça consiste em cada pessoa receber o que merece – isto é, receber a troca acordada – então cada indivíduo também define a justiça para si mesmo. A única restrição é a de que os acordos devem ser voluntários; ou seja, de que eles devem ser o que são: acordos.

> "O anarquismo e a liberdade não dizem nada sobre como as pessoas livres se comportarão ou sobre quais arranjos escolherão. Simplesmente diz que as pessoas têm a capacidade de escolher os arranjos que farão e quais os que não farão. O anarquismo não é normativo, ele não diz como se deve ser livre, mas apenas que a liberdade pode existir."
> – Karl Hess, "Anarchism Without Hyphens".

Sem a necessidade de consenso, várias versões da lei e da justiça podem e irão coexistir pacificamente dentro de um território. Elas podem funcionar diretamente ao lado um do outro ou dentro da mesma casa, e podem variar de contrato para contrato para a mesma pessoa, dependendo de seu propósito e de suas circunstâncias. Se alguém prefere a lei comum ocidental enquanto um vizinho judeu prefere a lei hassídica, que assim seja; ninguém está vinculado aos valores do outro, porque a execução de termos de uma pessoa de forma alguma impede a capacidade do outro de executar um conjunto diferente de termos. Os comunistas podem rejeitar uma cláusula politicamente censurável, como pagar aluguel, enquanto os capitalistas podem exigir que os contratos a incluam.

O código é a lei. A execução do código é justiça. Os indivíduos estão no controle.

Considere a dinâmica de um crime específico: A Fraude

O crime ainda existiria sob a justiça blockchain, pois sempre existirá em todas as sociedades, mas seria reduzido ao mínimo.

Um dos crimes privados contra os quais os usuários de criptomoedas exigem mais proteção é a fraude, que é uma forma de roubo. Certamente não é o único crime, mas examinar a fraude pode fornecer informações sobre como os outros podem ser tratados.

Roubo é a usurpação de propriedade sem o consentimento do proprietário; ou seja, nenhuma transferência de título acompanha a transferência real de um bem. Onde quer que a propriedade termine, o título permanece com o proprietário. Se a propriedade foi tomada por meio de violência direta, como num roubo, então ocorreu um assalto. Se foi obtida por meio de engano, o roubo é chamado de fraude. A fraude pode consistir em uma falsa troca de valor; uma pessoa vende um Rolex que é, na verdade, uma imitação barata, por exemplo. Ou a troca pode ocorrer em termos falsos; o Rolex genuíno acaba por ser uma propriedade roubada, sobre a qual o vendedor não tem nenhum título e nenhum direito de propriedade. O vendedor mente; o comprador acredita; o contrato de venda – explícito ou implícito – é inválido, pois a troca acordada não ocorreu. Não houve troca, apenas fraude.

Antes de discutir a fraude cripto, no entanto, é importante perceber que o crime pode não ser tão comum quanto muitos supõem.

A Australian Competition & Consumer Commission divulgou um relatório sobre o nível e os tipos de golpes que aconteceram em 2017. Fraudes relacionadas às criptomoedas constituíram 0,6% do total. Ou, como uma manchete da Panda Security afirmou recentemente:
“A fraude com criptomoedas é a exceção, não a regra.”

Para cada golpe, existem milhões de oportunidades que são criadas pela criptografia e pela blockchain para aumentar a riqueza e facilitar a cooperação entre os usuários. No entanto, cada caso de fraude chama mais atenção do que merece, porque as acusações são usadas para exigir regulamentação. Para exigir o envolvimento do estado.

Prestar atenção à fraude é necessário, é claro, mas o problema requer mais do que atenção. Requer uma diligência por parte dos usuários, que não pode ser legislada. Veja o golpe “mybtgwallet.com”, em 2017: O mybtgwallet.com ofereceu aos usuários carteiras Bitcoin Gold online gratuitas, através das quais eles poderiam verificar seus saldos e realizar transações gratuitas por um tempo limitado. A carteira era uma fraude, mas ganhou credibilidade ao aparecer brevemente no site oficial do Bitcoin Gold – um ato de extremo descuido, na melhor das hipóteses, por parte deste site. Para aceitar a oferta do mybtgwallet.com, os usuários precisavam enviar suas chaves privadas ou chaves de recuperação.

Um link fraudulento era um aspecto oculto do processo. Depois que usuários desavisados aceitaram a oferta da mybtgwallet, a criptomoeda em suas carteiras foi encaminhada para outros endereços: os endereços dos criminosos. De acordo com a Coindesk, "num elaborado esquema, mais de $3,3 milhões foram roubados de usuários de bitcoin, que buscavam reivindicar sua parte da criptomoeda recém-criada: a Bitcoin Gold. Pelo menos $30.000 em Ethereum, $72.000 em Litecoin, $107.000 em Bitcoin Gold e mais de $3 milhões em Bitcoin foram furtados."

Ninguém deveria ter caído nesse golpe porque ninguém deveria ter entregue suas chaves privadas, mas mesmo os veteranos das criptomoedas o fizeram. O fato de terem feito isso não significa que "eles mereciam"; esta não é a mensagem aqui. Uma pessoa com dinheiro transbordando de seus bolsos pode decidir dormir em um beco atrás do bar. Sua escolha é tola e perigosa, mas não o torna legalmente responsável se o dinheiro for roubado. Ela seria, ainda assim, vítima de um crime. Infelizmente, aqueles que entregam chaves privadas a estranhos fazem o equivalente a dormir em um beco com bolsos salientes. Essas pessoas seriam aconselhadas a desenvolver hábitos de advertência. Parte da propriedade em um mundo predatório é descentralizar a autodefesa, incluindo a defesa da propriedade.

Quais são algumas das lições a se aprender com o desastre do mybtgwallet.com para evitar fraudes? As especificidades incluem:

- Sempre assuma que um site estranho pode estar tentando roubar suas criptomoedas, sua identidade, seus dados ou todos esses itens. Estenda a confiança real somente após tomar as devidas precauções.
- Não lide com sites que exijam algo além das informações pessoais mais básicas. Prefira aqueles que incentivam o pseudonimato.
- Amigo ou não, nunca confie a ninguém seus dados privados ou suas chaves de recuperação. Isso equivale a divulgar a combinação de um cofre ou entregar um maço de dinheiro para alguém segurar enquanto você faz uma ligação. Dados e chaves de recuperação são a prova e o controle de propriedade. Eles constituem o título de propriedade da cripto.
- Nunca guarde seus dados ou chaves em qualquer lugar que seja vulnerável a ser copiado por outra pessoa.

- Sempre mantenha uma versão em papel de ambos em um local seguro como backup.
- Em essência, mantenha a privacidade. Os ladrões precisam de acesso para saquear. Não deixe suas portas abertas.

Essas são as especificidades. Mas esse é o ponto mais geral e fundamental: sempre tome as devidas precauções e sempre proteja a sua propriedade. Essas são as responsabilidades que advém da propriedade para o proprietário; as responsabilidades dos dados e dos usuários. Lembre-se: quando a criptomoeda sai de uma carteira, ela desaparece para sempre. Pelo menos essa deveria ser a sua suposição. A transação não pode ser revertida e poucas corretoras ou outros ramos da cripto oferecem seguro contra roubo. Até mesmo vítimas determinadas com casos documentados raramente recebem de volta mais do que alguns centavos de dólar, como as vítimas da Mt. Gox fizeram após anos e anos de exaustivo esforço.

Felizmente, a situação está mudando devido à necessidade de proteção do mercado. Um artigo de junho de 2019 no Zero Hedge comentou: “Os preços das criptomoedas foram atingidos da noite para o dia depois que a Binance, a maior corretora de criptomoedas do mundo, sediada em Hong Kong, revelou que hackers haviam fugido com 7.000 bitcoins – no valor de aproximadamente $41 milhões a preços atuais – roubados da ‘hot wallet’ da corretora. No entanto, os preços rapidamente reduziram algumas de suas perdas depois que a corretora anunciou que os clientes não seriam responsáveis pelas perdas: em vez disso, os depositantes seriam remediados com ativos da ‘Secure Asset Fund for Users’ da Binance.” E assim, a SAFU foi criada em 3 de julho de 2018, como uma resposta do mercado ao desejo de segurança dos usuários. A Binance aloca 10% do valor das taxas de trading realizadas em seu site e as transfere para um fundo de armazenamento em uma carteira fria para proteger os clientes em “casos extremos”.

Mecanismos de mercado e educação financeira minimizam os danos e eventos de fraude, possibilitando que pessoas desafortunadas ou descuidadas sejam protegidas. No entanto, é difícil proteger aqueles que correm para as criptomoedas por conta de FOMO (Fear Of Missing Out, medo de estar perdendo algo), assim como é difícil proteger aqueles que entregam suas economias nas mãos de estranhos contra o roubo. O crime sempre ocorrerá; o objetivo é reduzi-lo ao mínimo.

Quando a fraude ocorre, as pessoas clamam por regulamentação do governo. Mas há uma ironia sutil e amarga nessa dinâmica. Uma das razões pela qual as pessoas podem ser propensas à fraude é porque elas abordam a riqueza e os investimentos com uma mentalidade estatista. Ou seja: elas estão acostumadas às garantias de segurança do estado. Essas garantias são ilusões, mas isso não importa; o que importa para influenciar o comportamento das pessoas é que elas acreditem nas garantias. Nos EUA, por exemplo, a Federal Deposit Insurance Corporation garante o dinheiro que uma pessoa deposita em um banco até o valor de $250.000. A aplicação da lei opera divisões de fraude que registram relatórios do crime. Em suma, o estado faz com que as pessoas se sintam mais seguras do que deveriam, e isso as faz negligenciar as devidas precauções. O estado induz as pessoas a renunciar seu senso de responsabilidade.

A terceira parte confiável mais fraudulenta do mundo – o estado – não é um remédio. Suas falsas garantias vêm ao custo de sacrificar a privacidade e a liberdade individual, que são as maiores precauções de todas as riquezas. E, no fim, a riqueza ainda é saqueada.

Uma Revolução Prática e Descentralizada

A Revolução Satoshi está aqui e agora. É uma revolução prática, que é descentralizada ao nível individual.

Primeiro, a parte prática: a perfeição não é possível quando administrada por seres imperfeitos. Os criptoanarquistas que criaram o Bitcoin não eram apenas idealistas, mas também realistas; eles sabiam que o mundo e as criptomoedas nunca estariam perfeitamente a salvo da violência. O estado se intrometeria e as carteiras seriam hackeadas. Eles também sabiam que trabalhar em direção a um ideal é a única maneira de chegar o mais próximo possível dele. A situação é semelhante à ingestão diária de vitaminas: embora a saúde perfeita possa não ser alcançada, vitaminas e exercícios levarão alguém o mais próximo possível disso. E aproximar-se de ideais como a justiça é uma jornada que vale a pena, mesmo que o destino nunca seja alcançado.

O idealismo prático tem pelo menos dois benefícios utilitários. A rede de princípios para uma sociedade ideal é um mapa intelectual para avaliar se um ato específico se aproxima ou se afasta da liberdade. Se a liberdade de expressão é um dos princípios, por exemplo, suprimir um livro ofensivo afasta-se da liberdade e não deve ocorrer. Um ideal é

como o verdadeiro Norte em uma bússola. Ele diz: “Sim, esta é a direção correta”. A única coisa mais poderosa do que uma ideia cuja hora chegou é um *ideal* cuja hora chegou.

A descentralização: A Revolução Satoshi é uma revolução das expectativas crescentes; ela é impulsionada pelo desejo de liberdade, privacidade financeira e esperança para o futuro. A revolução está ocorrendo em uma base individual, porque não é mais necessário que as pessoas se levantem em massa, concordem com estratégias revolucionárias ou coordenem eventos por meio de comitês de terceiras partes confiáveis. Cada usuário se rebela sem drama ou ideologia enquanto persegue o interesse próprio, que é a motivação humana mais forte de todas. O interesse próprio em *todas* as suas formas deve ser a base de uma revolução bem-sucedida. Qualquer um que permaneça fiel à visão de Satoshi acerca das criptomoedas se manterá, quer queira ou não, como um lutador da liberdade, porque a descentralização radical do poder é a definição da Revolução, da nossa Revolução: da Revolução Satoshi.

O estado continua sendo o maior criminoso de todos; seu poder não deve ser subestimado, mas também não deve ser temido. A melhor atitude e abordagem em relação ao estado que já vi foi a do falecido Samuel E. Konkin III (SEK3), o pai do Agorismo e um velho companheiro de bebida. SEK3 atendia rotineiramente seu telefone com a saudação “Smash the State”; sua atitude em relação ao estado era infalivelmente rebelde. E, no entanto, sua atitude não era a abordagem prática que adotava em relação ao estado. Seu estilo de vida não enfatizava confrontos diretos com a autoridade; desafiar era sua atitude, não seu estilo de vida. Sempre que possível, SEK3 evitou contato e substituiu quaisquer serviços valiosos que o estado usurpou do livre mercado – como os bancos – com os privados. Suas ações eram um plano ambulante sobre como derrotar o estado eliminando-o de sua vida, porque ele sabia que a maneira mais eficaz de esmagar o estado era estabelecer alternativas privadas para torná-lo irrelevante, ou seja: privar o estado de sua vida privada.

O legado duradouro da SEK3 para a teoria anarquista foi o sistema econômico-filosófico chamado Agorismo, que busca uma revolução pacífica por meio da contra economia. SEK3 o definiu como “o estudo e prática de toda ação humana pacífica que é proibida pelo estado”. A contra economia é a versão “mercado negro” da praxeologia

de Mises, a qual Mises define como "o estudo da ação humana". O sistema de SEK3 é o estudo da ação humana necessária para negar a presença do estado na vida pessoal e na sociedade. Esmague o estado em atitude, substituindo-o na vida cotidiana. Não "esmague [literalmente] o estado"; apenas contorne-o.

SEK3 teria se deleitado com a audácia da criptomoeda que foi criada com a atitude "Smash the State", mas que adota a abordagem de evitar o confronto direto. Ele teria reconhecido imediatamente que estabelecer uma moeda melhor e de livre mercado é a maneira mais segura de enfraquecer a moeda fiduciária. Ele teria, com a mais absoluta certeza, declarado a criptomoeda "a moeda contra econômica" – a moeda do Agorismo. Mas mais do que isso. Em um piscar de olhos, o SEK3 teria reconhecido as implicações das criptomoedas para a justiça – exatamente porque elas evitam e substituem as leis estatais pelas do livre mercado, da privacidade e dos contratos. Em minha mente, consigo ver meu amigo Samuel tomando um gole da cerveja preta horrível que ele adora, seguido por uma tragada em seu cachimbo constantemente presente, antes de anunciar: "A anarquia chegou!"

Posfácio

Eu pretendia terminar este livro discutindo o impacto da blockchain na violência física, nos crimes de violência. Eu não posso. Não acho que haja impacto. Não sei como a blockchain poderia impedir estupros em becos, por exemplo. Eu poderia falar sobre colocar o trabalho sexual em um registro financeiro aberto, mas isso seria um chá fraco, e pareceria uma evasão. Este é um livro de teoria original, que explora o que nunca foi dito antes sobre criptomoedas. Nem sempre sei para onde as ideias estão me levando, mas o impacto na violência física não é um desses destinos.

E é por isso que estou, agora mesmo, escrevendo o posfácio do meu livro.

Minha jornada pelas criptomoedas começou em uma cozinha no Chile. Fui a palestrante de destaque em uma conferência, que também apresentou um painel de três outros especialistas em Bitcoin. Meu marido e eu decidimos alugar uma casa pelo AirBnb porque queríamos estender aqueles dois dias em duas semanas de saltos pelo país, o que foi mágico. A casa em que acabamos, no entanto, foi equipada para casamentos. Tradução: Havia cerca de trinta camas amontoadas em aproximadamente vinte quartos, que eram ligados por pisos feitos de compensado rachado, abaixo dos quais havia um desnível de dois andares. Não era uma casa; era uma aventura … com um banheiro funcionando. Eu prefiro chamá-la de exótica.

A conferência abrigou os palestrantes e atendentes em um complexo remoto, que rapidamente se encheu. Os organizadores nos pediram para receber os especialistas em Bitcoin. Nós concordamos com prazer. Eram sujeitos agradáveis e apresentáveis – embora homens que falavam de assuntos que não faziam sentido para mim. Felizmente, meu marido desenvolve hardware e software para sistemas embarcados, então estou acostumada a nem sempre entender as coisas.

E então houve a manhã depois que eles chegaram. Um sujeito dormiu até tarde. Um insistiu em preparar o café da manhã; não pretendo caluniá-lo, porque ele era muito agradável e tentava ser um bom hóspede. Mas as pessoas não cozinham perto de mim. Eu cozinho; você come; nos damos bem. Ele cozinhou…

Então, eu estava de mau humor quando olhei do outro lado da mesa do café da manhã para os olhos negros como carvão de Michael Goldstein, que mais tarde descobri ser fundador do Instituto Satoshi. Um jovem notável. Michael é apelidado de Bitstein por quem tem carinho por ele… e, sendo sincera, tudo que você precisa fazer é conhecê-lo para que isso aconteça. Quando olhei em seus olhos, tive uma sensação familiar, porque tenho espelhos no meu próprio banheiro. "Ele é um fanático", concluí. Acontece que gosto de fanáticos, dependendo do tópico em discussão, é claro. E eu não tinha nada contra as criptomoedas, que começaram a me interessar porque as pessoas que eu admirava as levavam muito a sério.

Com um olhar inabalável, Bitstein me disse que a blockchain era um registro financeiro aberto que daria luz à anarquia. Ok. Eu imediatamente entendi o poder da cripto para contornar o sistema bancário central… *se* fosse amplamente adotado; *se* não fosse proibido, *se*, Mas por que anarquia?

Todas as minhas ressalvas eram políticas e totalmente diferentes das de meu marido, que se juntou a nós depois de cerca de quinze minutos. Brad esperou até que Michael respirasse fundo e então disse uma palavra: "escalabilidade". Foi a primeira vez que Michael tropeçou. Ele disse: "estamos trabalhando nisso". Eu vi Brad perder algum interesse.

Mas eu não. Eu não sabia o que escalabilidade significava nesse contexto, exceto no senso comum. Mas eu não me importei porque a palavra "anarquia" tinha sido pronunciada, e isso eu sabia. Michael parecia mais do que feliz em abandonar a escalabilidade para a política, e eu investiguei por que ele achava que o alvorecer da liberdade havia chegado como uma cavalaria em um algoritmo.

Michael respondeu, e não me convenceu, mas me instigou a ler. Assim como meu velho amigo Jeff Tucker. Assim como o incrível Stephan Kinsella. Outras pessoas tentaram aumentar minha consciência também. Mihai Alisie, da *Bitcoin Magazine*, me pediu para escrever para ele sobre o anarquismo, por exemplo. Acho que não agradeci adequadamente a ele por ter tanta confiança em mim. E naquele ponto, sua confiança provavelmente era infundada. Enviei um artigo para a Bitcoin Magazine, que estava longe de ser o meu melhor trabalho. Isso atraiu uma resposta melhor do que eu merecia: eles estavam dispostos a "trabalhar comigo". Agradeci ao editor e recuei com a desculpa absolutamente genuína de que não sabia se tinha algo original para contribuir para a discussão. Eu não tinha nada de novo para dizer. Eu ainda não

tinha entendido as arestas duras e frias da teoria cripto e não entendia seu poder. O que significava que eu ainda não tinha demarcado a única área onde eu poderia e posso contribuir com algo original: a integração do criptoanarquismo com a rica história da teoria anarquista-libertária que se estende por séculos.

À medida que lia mais, fiquei envergonhada de mim mesma. Criptoanarquismo: o desenvolvimento político mais importante da minha vida ocorreu sem que eu percebesse, o que é imperdoável. Eu havia gastado meu tempo com o libertarianismo "oficial" – institutos orientados por doações e definidos por doações, universidades financiadas por impostos, revistas acadêmicas. Quando foi que a liberdade chegou embalada em dólares de impostos, prêmios e homenagens entregues em jantares beneficentes? A liberdade é uma luta de rua. O criptoanarquismo tomou as ruas sem que eu percebesse. Mas agora eu o vejo.

Roger Ver. Nosso primeiro contato foi um e-mail que ele enviou do nada. O e-mail de Roger me conquistou de primeira, porque ele usou a palavra "voluntarismo". Em 1982, fui uma das três pessoas que criaram o movimento voluntarista moderno durante uma conversa fiada, em um apartamento de dois quartos com aluguel recente em Hollywood, Califórnia. Lembro-me de meus dedos literalmente zumbindo com a excitação das ideias e planos que estávamos forjando na época: Carl Watner, George H. Smith e eu. Mas, principalmente, Carl. Era e é quase inacreditável para mim que, décadas e décadas depois, um visionário voluntarista chamado Roger estivesse batendo à minha porta (por assim dizer). Ele me pediu para escrever para seu site.

Roger teve um bom timing. Em linguagem de ficção científica, eu finalmente *grokkei* (entendi) o bitcoin; Além disso, tiro meu chapéu para Robert A. Heinlein por inventar essa palavra. E tiro meu chapéu para Roger e toda a equipe do bitcoin.com por nunca – e quero dizer, nem uma vez, de qualquer maneira – terem tentado influenciar minhas ideias enquanto eu as desenvolvia nas minhas tentativas (às vezes desajeitadas) de integrar o criptoanarquismo nas tradições mais amplas do liberalismo clássico, da economia austríaca e do anarquismo individualista.

A montagem do livro se transformou em uma reescrita maciça, seguida por um período de edição feroz. O livro diante de você agora é baseado nas colunas que eu serializei no bitcoin.com, mas pelo menos metade do material é novo – especialmente a seção sobre justiça.

Antes de encerrar, devo abordar outro aspecto do criptoanarquismo. Eu não esperava esse efeito colateral benéfico, mas aí está ele; a vida é muitas vezes inesperada. O mundo cripto me fez jovem novamente.

Tive a imensa sorte de fazer amizade e passar muitos anos com pessoas que ajudaram a fundar o movimento libertário. Murray Rothbard costumava brincar, nas conferências de 1980, dizendo que o libertarianismo poderia ser eliminado por uma bomba bem colocada. Ele estava certo, mas agora o movimento é imenso. Vão precisar de uma bomba maior.

Ainda assim, há uma desvantagem para toda essa minha sorte: as pessoas com quem cresci na intelectualidade adulta agora me fazem sentir velha, principalmente porque muitas delas estão mortas; eu geralmente era a mais nova na sala. Sentir-se velho é sentir-se cansado, sem nada à vista que faça seus olhos brilharem.

Lembro-me de Murray e de sua paixão– lembro-me tão vividamente …, Mas, ao longo dos anos, algo deu errado com sua paixão. Veio da raiva, eu acho, e se expressou atacando outras pessoas. Lembro-me de um jantar pós-conferência em que um colega teve a infelicidade de dizer algo positivo sobre Keynes. E então – Deus nos ajude! – ele elaborou. Murray finalmente explodiu em um discurso retórico com sua voz chiada broklinesca, e o sujeito começou a recuar. Acho que ele teria empurrado sua cadeira para fora do restaurante, se essa fosse uma possibilidade. O colega admitiu que Keynes podia estar errado sobre "esta" questão, e sobre "aquela" questão. E que, provavelmente, Keynes poderia ser considerado "fraco" no contexto histórico. Murray desceu a mão aberta sobre a mesa e disse em voz alta: "E Hitler foi 'fraco' com os judeus!". Todos rimos, embora sabendo que aquilo havia sido um ataque… e um aviso.

A cripto brilha como uma coisa girando ao sol; e o brilho é limpo, porque não vem da raiva ou de humilhação de alguém ou qualquer coisa parecida. A paixão que vem dela é positiva. Uma porta se abriu, e não sei onde o caminho que ela mostra me levará, porque nunca poderia ter previsto até onde cheguei. Que os tijolos amarelos sejam gentis comigo.

Uma coisa eu sei: estou em boa companhia; a crew do bitcoin.com não foi nada menos que decente e sorridente para essa mulher que ousou se intrometer em seu mundo. Isso significa muito para mim. Não sei onde vou parar em seguida, mas sei que a tecnologia – e não apenas as criptos – vai nos dar uma aventura selvagem pelo resto de nossas vidas.

Minhas mãos estarão sobre o teclado, dedicadas a colocar as mudanças corriqueiras em perspectiva histórica, mesmo enquanto elas estiverem acontecendo.

Eu tenho uma chance de fazer isso … porque eu sou jovem novamente; estou esperançosa. E nada, nada é impossível. Foi isso que este livro significou para mim. Faço uma pausa nesta jornada, neste exato momento, para te agradecer por fazer parte dela:

Seja bem-vindo à Revolução Satoshi.